AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (CFATS) PROGRAM: A PROGRESS UPDATE

HEARING

BEFORE THE

SUBCOMMITTEE ON ENVIRONMENT AND THE ECONOMY

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

MARCH 14, 2013

Serial No. 113–15

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE
80–377 WASHINGTON : 2013

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

RALPH M. HALL, Texas
JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Missouri
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York

SUBCOMMITTEE ON ENVIRONMENT AND ECONOMY

JOHN SHIMKUS, Illinois
Chairman

PHIL GINGREY, Georgia
Vice Chairman
RALPH M. HALL, Texas
ED WHITFIELD, Kentucky
JOSEPH R. PITTS, Pennsylvania
TIM MURPHY, Pennsylvania
ROBERT E. LATTA, Ohio
GREGG HARPER, Mississippi
BILL CASSIDY, Louisiana
DAVID B. MCKINLEY, West Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Missouri
JOE BARTON, Texas
FRED UPTON, Michigan, *ex officio*

PAUL TONKO, New York
Ranking Member
FRANK PALLONE, JR., New Jersey
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
JERRY MCNERNEY, California
JOHN D. DINGELL, Michigan
JANICE D. SCHAKOWSKY, Illinois
JOHN BARROW, Georgia
DORIS O. MATSUI, California
HENRY A. WAXMAN, California, *ex officio*

CONTENTS

	Page
Hon. John Shimkus, a Representative in Congress from the State of Illinois, opening statement	1
Prepared statement	2
Hon. Paul Tonko, a Representative in Congress from the State of New York, opening statement	2
Hon. Henry A. Waxman, a Representative in Congress from the State of California, prepared statement	113

WITNESSES

Rand Beers, Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security	5
Prepared statement	7
Answers to submitted questions	117
David Wulf, Director, Infrastructure Security Compliance Division, U.S. Department of Homeland Security	14
Prepared statement	7
Answers to submitted questions	117
Stephen L. Caldwell, Director, Homeland Security and Justice, Government Accountability Office	34
Prepared statement	36
Answers to submitted questions	143
William E. Allmond, IV, Vice President, Society of Chemical Manufacturers and Affiliates	63
Prepared statement	65
Answers to submitted questions	149
Timothy J. Scott, Chief Security Officer and Corporate Director, the Dow Chemical Company, on Behalf of the American Chemistry Council	71
Prepared statement	73
Answers to submitted questions	157
Charlie Drevna, President, American Fuel and Petrochemical Manufacturers	78
Prepared statement	80
Answers to submitted questions	168
Rick Hind, Legislative Director, Greenpeace	86
Prepared statement	88
Answers to submitted questions	175

SUBMITTED MATERIAL

Letter of March 12, 2013, from the National Association of Chemical Distributors to Mssrs. Shimkus and Tonko	117

CHEMICAL FACILITY ANTI–TERRORISM STANDARDS (CFATS) PROGRAM: A PROGRESS UPDATE

THURSDAY, MARCH 14, 2013

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ENVIRONMENT AND ECONOMY,
COMMITTEE ON ENERGY AND COMMERCE
Washington, DC.

The subcommittee met, pursuant to call, at 10:07 a.m., in room 2322 of the Rayburn House Office Building, Hon. John Shimkus (chairman of the subcommittee) presiding.

Members present: Representatives Shimkus, Pitts, Murphy, Latta, Harper, Cassidy, McKinley, Bilirakis, Johnson, Barton, Tonko, Green, Schakowsky, McNerney, Barrow ,and Waxman (ex officio).

Staff present: Nick Abraham, Legislative Clerk; Charlotte Baker, Press Secretary; Matt Bravo, Professional Staff Member; Jerry Couri, Senior Environmental Policy Advisor; David McCarthy, Chief Counsel, Environment and the Economy; Chris Sarley, Policy Coordinator, Environment and the Economy; Tom Wilbur, Digital Media Advisor; Jacqueline Cohen, Democratic Counsel; Greg Dotson, Democratic Staff Director, Energy and Environment; and Caitlin Haberman, Democratic Policy Analyst.

OPENING STATEMENT OF HON. JOHN SHIMKUS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. SHIMKUS. I would like to call the hearing to order.

We want to welcome our first panel, and I would like to recognize myself for 5 minutes for an opening statement.

Good morning. The Subcommittee is now in order and I want to recognize myself for 5 minutes. Today marks the fourth hearing we have had on CFATS and the third consecutive one we have had since I became the subcommittee chairman.

Sadly, it has been a very painful process to see how badly CFATS had fallen short of our expectations and to see the struggle, both inside of DHS as well as externally, to get the program back on track. There are some positive reports about progress from DHS, GAO, and the regulated stakeholders, but we have uncovered more details showing that in key areas the suggested progress is not what we had hoped. I think strides have been made to remedy many of the managerial concerns of 1 year ago, and some of our testimony will suggest communication lines have been opened in a way that could lead to longer-term achievements for the program.

By many accounts, Infrastructure Security Compliance Division Director David Wulf deserves a great deal of credit. Mr. Wulf, we appreciate your tireless, consistent, candid, and long-standing commitment to improving CFATS when others could not. I also think this process is merely meant to get us back to a semi-functional program, not a perfect or fully implemented program.

Unfortunately, underlying programmatic issues we discussed in the last hearing—such as the fact that CFATS risk assessment falls far short of DHS' own National Infrastructure Protection Plan and the CFATS regulations, and the long time frame for evaluating Site Security Plans, despite the incomplete risk assessment—continue to threaten the credibility of the program not only on the Hill, but with regulated stakeholders who are confused by many decisions made within the program.

As Chairman Upton has said before to DHS, we are all on the same side. The enemy here is the terrorists who would seek to harm our Nation. We need to work together to determine the best path forward for CFATS and its reauthorization, but we can't do so if we aren't fully informed and in a way that verifies the details coming forward. That is why we are going to have some tough and balanced assessment of the program delivered by DHS, the Government Accountability Office, and the CFATS stakeholder community.

Our witnesses today may not tell us exactly what we want to hear, but they will tell us what we need to know. I want to thank all of these witnesses for appearing before our panel here today. I believe we are at a critical juncture for the success of the CFATS program in that the internal issues distracting the program are not our focus, but rather getting the program right, functioning effectively, efficiently, as Congress drafted the law. Their perspective will be crucial in getting serious questions answered by the program and our ability to work together.

[The prepared statement of Mr. Shimkus follows:]

PREPARED STATEMENT OF HON. JOHN SHIMKUS

Today marks the fourth hearing we have had on CFATS, and the third consecutive one we have had since I became subcommittee Chairman.

Sadly, it has been a very painful process to see how badly CFATS had fallen short of our expectations and to see the struggle, both inside DHS as well as externally, to get the program back on track. There are some positive reports about progress from DHS, GAO and the regulated stakeholders, but we've uncovered more details showing that in key areas the suggested progress is not what we had hoped.

I think strides have been made to remedy many of the managerial concerns of one year ago and some of our testimony will suggest communication lines have been opened in a way that could lead to longer term achievements for the program. By many accounts, Infrastructure Security Compliance Division (ISCD) Director David Wulf deserves a good deal of credit. Mr. Wulf, we appreciate your tireless, consistent, candid, and long-standing commitment to improving CFATS when others could not.

I also think this progress is merely meant to get us back to a semi-functional program, not a perfect or fully implemented program. Unfortunately, underlying programmatic issues we discussed in the last hearing—such as the fact that CFATS risk assessment falls far short of DHS's own National Infrastructure Protection Plan and the CFATS regulations, and the long time frame for evaluating site security plans, despite the incomplete risk assessment—continue to threaten the credibility of the program not only on the Hill, but with regulated stakeholders who are confused by many decisions made within the program.

As Chairman Upton has said before to DHS, we are all on the same side, the enemy here is the terrorists who would seek to do harm to our nation. We need to work together to determine the best path forward for CFATS and its reauthorization, but we can't do so if we aren't fully informed and in a way that verifies the details coming forward. That's why we are going to have some tough but balanced assessments of the program delivered by DHS, the Government Accountability Office, and the CFATS stakeholder community.

Our witnesses today may not tell us exactly what we want to hear, but they will tell us what we need to know. I want to thank all of these witnesses for appearing before our panel here today.

I believe we are at a critical juncture for the success of the CFATS program, in that the internal issues distracting the program are not now our focus, but rather getting the program right, functioning effectively, efficiently, as congress drafted the law. Their perspective will be crucial to getting serious questionsanswered by the program and our ability to work together.

# # #

Mr. SHIMKUS. And with that I would like to yield 1 minute to the gentleman from Texas, Mr. Barton.

Mr. BARTON. Thank you, Mr. Chairman, for holding this hearing today.

Two years in a row this subcommittee has convened a hearing to discuss the concerns with the CFATS program. Last year, we became aware of an internal DHS memorandum which detailed an array of management flaws and achievement gaps with that program. One of the witnesses today was a co-author. When news of these problems surfaced, several Members of Congress, including myself, asked the GAO to determine what actions DHS was taking to address the problems. We learned in the GAO report that resulted of a 94-item Action Plan that DHS developed to address those various issues. I understand today that the most egregious examples of waste of taxpayer dollars have been addressed but there is still work to do. We are at a critical juncture.

DHS has been reviewing information since 2007 by operators of over 40,000 facilities. By January of this year, they had identified about 4,400 as high-risk facilities. Of those, about 90 percent were tier-based on the risk that they presented—meaning that they would have to submit Site Security Plans for DHS review. We now know that there have been significant errors in the risk assessment methodology. We also know that only a few dozen of the 3,100 high-risk security plans have been reviewed and approved. There is much work to be done. I hope this hearing will facilitate some of that work.

Thank you for the hearing and thank you for the time and I yield back.

Mr. SHIMKUS. The gentleman yields back his time.

The chair now recognizes the ranking member of the subcommittee, Mr. Tonko, for 5 minutes.

OPENING STATEMENT OF HON. PAUL TONKO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Mr. TONKO. Thank you. Thank you, Mr. Chairman. And good morning and thank you to our chair for convening this hearing and certainly to our witnesses for participating today and providing your insight and offering very important information.

Ensuring the safety of our citizens and avoiding serious disruption of our economy requires us to remain vigilant and to anticipate potential targets and actions of violent individuals and groups. The goal of the Chemical Facility Anti-Terrorism Standards, the CFATS program, is to ensure that chemical facilities have robust plans to prevent terrorists from sabotaging them and to minimize the impacts should that prevention fail.

Two years ago, an internal memorandum revealed serious problems with the CFATS program. While some progress has been made to address some of the shortcomings, there is still much more work to be done. That work surely falls to the Department of Homeland Security, clearly having more work to do, but also it falls to Congress. Congress created the Department of Homeland Security in 2002 and charged DHS with coordinating federal policy to protect this Nation's critical infrastructure. This is a complex task involving not only the Federal Government but a partnership with state and local governments, as well as the private sector.

Congress defined this complex and essential task of protecting chemical facilities with a paragraph in an appropriations bill. The deficiencies in this program are partly a reflection of our failure to come together and provide clear guidance to the administration.

The industry has been active in this area. They have taken many steps through initiatives such as the Responsible Care Program to develop and disseminate best practices to member companies of industry organizations. These programs are, however, voluntary. Private industry does not have the tools of surveillance and intelligence as that which the Federal Government has. In order to be most effective, we must have partnerships working together and the program must have the public's confidence that their communities are indeed safe. The public and the industry will benefit from a federal program that is developed with their input and in which standards, practices, and policies are defined clearly by the Department of Homeland Security.

The CFATS program is not the only federal program regulating chemical facilities. Other federal departments and agencies have programs with longer histories and well-established protocols. There should be a consultation amongst federal agencies to apply best practices, identify gaps in responsibility, and to avoid conflicting regulations and policies.

I hope this will not be the last hearing on this issue. This committee should develop legislation that provides clear direction to DHS, certainty to the regulated industry, and confidence to the public that the CFATS program is providing the protection we require and deserve. A paragraph in an appropriations bill that must be renewed annually simply does not meet those needs.

I would like to thank all of our witnesses for appearing before us today. I look forward to your testimony and to hearing your views on how we can improve this most essential program.

With that, I thank you. Mr. Chairman, I yield back.

Mr. SHIMKUS. I want to thank my colleague. And I can guarantee it will not be last hearing on this issue, and we would like to authorize a program.

So with that, I would like to turn to my colleagues on my side and ask if anyone would like to submit an opening statement.

Seeing none, I turn to your side. No one? Thank you very much.

Now, I would like to recognize Mr. Rand Beers, the Under Secretary for the National Protection and Programs Directorate of the United States Department of Homeland Security.

Sir, your full statement is in the record. You are recognized for 5 minutes.

STATEMENT OF HON. RAND BEERS, UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY; AND DAVID WULF, DIRECTOR, INFRASTRUCTURE SECURITY COMPLIANCE DIVISION, U.S. DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF HON. RAND BEERS

Mr. BEERS. Thank you, Chairman Shimkus and Ranking Member Tonko and other members of the committee. I appreciate the opportunity to be before you today to talk about the Department's regulation of high-risk chemical facilities.

Let me start by emphasizing that the CFATS program has already made the Nation more secure. The program has identified high-risk chemical facilities across the country. It has provided them with the tools to identify their vulnerabilities, and it has helped them to develop plans to reduce the risks associated with these chemicals.

Since its inception, CFATS has helped 3,000 chemical facilities eliminate, reduce, or otherwise modify their holdings so that they no longer possess potentially dangerous chemicals and are no longer considered high-risk. The significant reduction in the number of chemical facilities that represent the highest risk is an important success of the CFATS program and is attributable both to the design of the program as enacted by Congress and to the work of the CFATS personnel and industry at the thousands of chemical facilities that we work with on a regular basis.

Over the past year, NPPD has worked diligently to turn a corner and has addressed many of the challenges identified by the program's leadership. The CFATS program has made significant progress advancing programmatically while simultaneously addressing the internal operational concerns. Equally important, the Department remains committed to working with stakeholders and with the Congress on a path forward to ensure that the CFATS program continues to build upon the successes to date.

Over the last 6 months ISCD has made considerable progress in conducting authorization inspections and approving Site Security Plans. When I was here in September, we had authorized 73 Site Security Plans. Today, we have authorized 261. That is a 400 percent increase. In September we had conducted 19 authorization inspections; today, we have conducted 141. That is a 700 percent increase. In September we had approved only two Site Security Plans; now, we have approved 52, including 3 Alternative Security Programs.

While these are significant achievements in the last 6 months, we recognize that we need to do much more and we need to increase the pace at which we are doing it. And we are looking at potential approaches for increasing the pace of security plan re-

views and inspections for the lower Tier 3 and Tier 4 facilities without sacrificing quality and consistency.

NPPD will work with the regulated community to gather feedback and thoughts on how best to increase the pace of the lower tiers. For example, we have been looking with industry on the development of templates, or corporate alternative Security Programs, and we believe that the use of ASPs will significantly increase the pace and improve our security plans. We have also discussed ASPs with the Coast Guard and will apply the lessons that they have learned regarding their use of ASPs to take your point, Ranking Member Tonko, about talking to our partners who also have regulatory programs.

Regarding our private sector partners, the Department has received primarily positive feedback on outreach and communications efforts from the regulated community. And we will continue to address specific areas of interest to the CFATS community. For instance, recognizing that regulated facilities best understand their risk drivers and in support of increased transparency, the Department is analyzing what aspects of the classified risk tiering methodology it can and should share with members of the regulated community. In fact, that particular question has been presented to the risk methodology external Peer Review Panel for analysis. And I might add that this is a peer review that includes private sector participation. And the Department is looking forward very much to the panel's recommendations with respect to this.

The Department has also actively engaged stakeholders regarding personnel surety. During the last 6 months, we have been listening to stakeholder feedback on personnel surety and we have revised our program based on this feedback. We now believe we have a proposal which provides the regulated community with flexibility for carrying out the outstanding requirement for personnel surety and reflects input from facilities of all sizes. This proposal balances the need to conduct thorough vetting of personnel for national security purposes with a desire to minimize the burden on facilities. Our engagement with the private sector will be reflected in two department Notices that have gone from the Department to the Federal Register and will be published in the coming days.

I close with a note regarding the Department's current statutory authority to implement CFATS. As you are aware, the CFATS authorization currently extends through March 27 of this year. The Department supports a permanent authorization for the CFATS program and we are committed to working with the Congress and other security partners to establish a permanent authority for the CFATS program in federal law. Overall, I am here before you today convinced that we have positioned the program firmly on the right track and I would be happy to respond to any questions that you may have.

Thank you.

[The prepared statement of Mr. Beers and Mr. Wulf follows:]

Statement for the Record

Under Secretary Rand Beers
National Protection and Programs Directorate
Department of Homeland Security

Director David Wulf
National Protection and Programs Directorate
Department of Homeland Security

Before the
Committee on Energy and Commerce
Subcommittee on Environment and the Economy
United States House of Representatives

March 14, 2013

Thank you, Chairman Shimkus, Ranking Member Tonko, and distinguished Members of the Committee. I appreciate the opportunity to appear before you today to discuss the Department of Homeland Security's (DHS) regulation of high-risk chemical facilities under the Chemical Facility Anti-Terrorism Standards (CFATS). Over the past year, NPPD has worked diligently to turn a corner and has addressed many issues previously identified as challenges. The CFATS program has made significant progress, advancing programmatically while simultaneously addressing internal operational concerns. The Department remains committed to working with stakeholders and with Congress on a path forward so that the CFATS program continues to improve. My testimony today focuses on the progress made since our last hearing, the current status of the program, and upcoming activities.

The CFATS program has made our Nation more secure by identifying and regulating high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with these chemicals. CFATS has also played a role in reducing the number of high-risk chemicals, as close to 3,000 facilities have eliminated, reduced or modified their holdings of certain chemicals. We welcome the opportunity to work with stakeholders to further improve this vital national security program. As the Directorate with oversight responsibility for the CFATS program, NPPD, and the Directorate's Infrastructure Security Compliance Division (ISCD), is continually evaluating the program to identify areas for improvement to ensure proper implementation of the program. Through ISCD's comprehensive Action Plan, we have identified and acted decisively to address areas in which improvements were warranted.

As you are aware, the Department's current statutory authority to implement CFATS – Section 550 of the fiscal year (FY) 2007 Department of Homeland Security Appropriations Act, as amended – currently extends through March 27, 2013. DHS recognizes the significant work that the Subcommittee and others have accomplished to reauthorize the CFATS program. The Department supports a permanent authorization for the CFATS program and is committed to working with Congress and other security partners to establish a permanent authority for the CFATS program in Federal law.

CFATS Implementation Progress

The CFATS program has already made our Nation more secure by identifying and regulating high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with these chemicals. The cornerstone of the CFATS program in regulating the security of high-risk chemical facilities is the development, submission, and implementation of Site Security Plans (SSPs), which document the facility security measures that satisfy the applicable Risk-Based Performance Standards (RBPS) under CFATS. It is important to note that these plans are not "one size fits all," but in-depth, highly customized, and dependent on each facility's unique circumstances. Following a facility's development and submission of an SSP, ISCD conducts an authorization inspection that is tailored to review specific details within the facility's SSP. High-risk facilities also have the option of submitting an Alternative Security Program (ASP) in lieu of an SSP. Over the last six months, ISCD has made significant strides in authorizing SSPs and ASPs, conducting Authorization Inspections, and approving security plans. NPPD recognizes the need to increase the pace of authorization and approvals and is examining potential approaches for increasing the pace of SSP reviews and inspections for the lower risk Tier 3 and Tier 4 facilities without sacrificing quality or consistency.

Tier*	Total # of Facilities	Received Final Tier	Authorized SSPs and ASPs	Authorization Inspection Conducted	Approved SSPs and ASPs
1	131	117	83	61	36
2	450	398	172	68	4

*As of March 5, 2013

In order to determine whether a facility is regulated under CFATS, the facility uses the web-based Chemical Security Assessment Tool (CSAT), to submit a Top-Screen to ISCD. Since we began collecting this information in 2007 ISCD now has data from more than 44,000 Top-Screens submitted by chemical facilities, providing important information about their chemical holdings. Based on the information received in the Top-Screens, ISCD identified more than 8,500 facilities that were initially designated as high-risk facilities potentially regulated by CFATS. These facilities then compiled and submitted Security Vulnerability Assessments, which are used by ISCD to identify which facilities present a terrorism risk that is sufficiently high to warrant the assignment of a final high-risk tier under CFATS.

As of March 5, 2013, CFATS covers 4,380 high-risk facilities nationwide; of these, 3,468 have received final high-risk determinations and are required to develop SSPs (or ASPs) for ISCD review. The remaining facilities are awaiting final tier determinations based on their Security Vulnerability Assessment submissions. ISCD continues to issue final tier notifications to facilities across all four risk tiers. Facilities that receive a final high-risk determination are notified of the requirement to complete and submit an SSP or an ASP. Tiering determinations are dynamic and can change based on actions a facility takes. For example, a tiering determination can change when a facility voluntarily alters its operations in a material way that reduces its risk profile. Since the inception of CFATS, close to 3,000 chemical facilities have eliminated, reduced, or otherwise made modifications to their holdings of potentially dangerous chemicals and are now no longer considered high-risk. The significant reduction in the number of chemical facilities that represent the highest risk is an important success of the CFATS

program and is attributable both to the design of the program as enacted by Congress and to the work of CFATS personnel and industry at thousands of chemical facilities.

Site Security Plans. Among the important items identified in the ISCD Action Plan was the need to streamline the process for reviewing SSPs. This has enabled the program to complete SSP reviews, authorizations, and approvals for Tier 1 and 2 facilities at an accelerated pace. In the first months of 2012, ISCD took an operational pause as it developed a refined approach to SSP reviews—one that eliminates bottlenecks and involves field inspectors (who work most closely with CFATS facilities) early on in the process. This effort has enabled the program to accelerate the pace of SSP reviews, authorizations, and approvals for Tier 1 and 2 facilities. To date, ISCD has completed its review of all Tier 1 SSPs and has begun reviewing Tier 2 SSPs. ISCD anticipates that we will have completed the approval process for all Tier 1 security plans by October 2013 and for all Tier 2 security plans by May 2014.

Inspections. ISCD is currently carrying out authorization inspections for Tiers 1 and 2 facilities. Authorization inspections are scheduled after ISCD's review of an SSP (or ASP) results in a preliminary determination that the SSP satisfies applicable RBPS and issues a Letter of Authorization. Since resuming authorization inspections in July 2012, ISCD has conducted 120 authorization inspections. The authorization inspection results, as well as any further revisions that the facility may make to the SSP (or ASP), are reviewed to make a final determination as to whether the facility's SSP satisfies the applicable RBPS and whether to issue a Letter of Approval. Once issued a Letter of Approval, the facility's SSP (or ASP) is considered approved and the facility must implement the security measures detailed in the SSP. ISCD plans to conduct compliance inspections approximately one year after an SSP approval, therefore the first compliance inspections will take place around September 2013.

Alternative Security Plans. ASPs are an important part of the CFATS program's continued progress and its effort to streamline the authorization and inspection process. The ASP provides an option for regulated facilities to submit information necessary to document site security measures that address the RBPS through a format other than the SSP template. ISCD has been working closely with industry stakeholders regarding options for their development and use of ASPs. Recently, the American Chemistry Council released a guidance document and template developed in consultation with DHS to assist its members with the development of ASPs. Additionally, DHS has been in discussion with other industry stakeholders, including the Agricultural Retailers Association and the Society of Chemical Manufacturers Affiliates, about developing templates. DHS has also been engaging industry on the development of "corporate" ASPs. For members of industry that own several regulated facilities, the corporation can develop a single ASP, which can be easily replicated by other facilities. ASPs submitted by facilities using any industry-developed or proprietary template would be reviewed under the same standards that ISCD currently reviews SSPs. The potential for these ASPs to serve as a force multiplier is tremendous.

Compliance Assistance and Facility Outreach. Compliance Assistance Visits provide chemical facilities with support in preparing for the necessary security-related documentation required by CFATS. During these visits, ISCD offers compliance and technical assistance in the completion of the CSAT registration, Top Screen, Security Vulnerability Assessment, or Site Security Plan. At any point in the CFATS process, a facility can request a Compliance

Assistance Visit. As of March 5, 2013, ISCD has conducted more than 1,080 Compliance Assistance Visits. In addition to conducting inspections and supporting Compliance Assistance Visits at regulated facilities, NPPD's Chemical Security Inspectors actively work with facilities, local stakeholders, and governmental agencies across the country. Collectively, they have participated in more than 5,000 meetings with Federal, state, and local officials; held more than 4,600 introductory meetings with owners and operators of CFATS-regulated or potentially regulated facilities.

Industry Engagement and Information Sharing. Since the establishment of the CFATS program in April 2007, NPPD has conducted significant outreach to the regulated community and other interested or affected entities so that they are aware of the program's requirements. NPPD and ISCD management and staff have presented at hundreds of security and chemical industry gatherings and participated in a variety of other meetings. As part of this outreach initiative, NPPD and ISCD leadership have regularly updated affected sectors through their Sector Coordinating Councils and the Government Coordinating Councils—including the Chemical, Oil and Natural Gas, and Food and Agriculture Sectors. To promote information sharing, ISCD has developed several communication tools for stakeholder use, including: the Chemical Security website (www.DHS.gov/chemicalsecurity); a help desk for CFATS-related questions; a CFATS tip-line for anonymous chemical security reporting; and CFATS-Share, a web-based information-sharing portal that provides certain Federal, state, and local agencies access to key details on CFATS facility information as needed.

Intergovernmental Coordination. NPPD continues to collaborate within DHS and with other Federal agencies in the area of chemical security, including routine engagement with the U.S. Coast Guard (USCG); the Transportation Security Administration (TSA); the Department of Justice's Federal Bureau of Investigation (FBI) and Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); the Nuclear Regulatory Commission (NRC); and the Environmental Protection Agency (EPA). In December, the USCG and NPPD signed a Memorandum of Agreement authorizing sharing data and risk methodologies between ISCD's Chemical Security Assessment Tool and USCG's Maritime Security Risk Analysis Model. The data sharing will help provide greater visibility to both USCG and ISCD with regard to how each organization assesses and quantifies risk and ultimately will support the development of a comprehensive risk picture for facilities within the Chemical Sector and aid in the identification of potentially unacceptable security gaps that may require changes in regulation or policy.

Personnel Surety. Under CFATS Risk-Based Performance Standard 12 (RBPS 12), final high-risk chemical facilities are required to perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets. These include: (i) measures designed to verify and validate identity; (ii) measures designed to check criminal history; (iii) measures designed to verify and validate legal authorization to work; and (iv) measures designed to identify people with terrorist ties. The Department currently reviews, authorizes and approves facility SSP/ASP submissions for RBPS-12 (i), (ii), and (iii). To collect information to fulfill RBPS-12 (iv), NPPD previously submitted to OMB an Information Collection Request in June 2011, but withdrew the Request in order for the Department to further engage with our security partners and with stakeholders in the regulated community about the CFATS Personnel Surety Program given their concerns about the proposed collection.

Over the past six months, the Department invited 25 industry associations to participate in CFATS Personnel Surety conference calls and subsequently held calls with 16 of the organizations. NPPD also met five times with the Sector Coordinating Council leadership and members to identify their primary issues of concern with the CFATS Personnel Surety Program, to discuss privacy-related issues, and to review how use of third parties could be leveraged to provide additional options for facilities to ensure vetting of facility personnel and unescorted facility visitors. We have also engaged a coalition of associations about their concerns related to the transportation sector. Finally, in January, NPPD held a meeting in coordination with the FBI, the Oil & Natural Gas Sector Coordinating Council, and the Chemical Sector Coordinating Council to discuss coordinated U.S. Government response and law-enforcement-investigative activity that may occur in the event of a positive match against the terrorist screening database. We have worked to incorporate this feedback into the revised personnel surety program, and expect to publish a 60-day notice to solicit comment about the proposed information collection in the Federal Register in the next week. After that, the Department plans to concurrently publish a 30-day Federal Register notice to solicit additional comments, and submit a new Information Collection Request for the CFATS Personnel Surety Program to the Office of Management and Budget. Our 30-day notice in the Federal Register will also respond to all comments we receive from the 60 day Federal Register notice. The Department is committed to finalizing the outstanding aspect of personnel surety and implementing a program that provides flexibility to facilities as the final piece to the overarching chemical security program.

Risk Assessment Methodology Review. NPPD is committed to conducting a thorough review of the risk assessment process and keeping Congress apprised of any significant issues related to that review. In support of this, NPPD has implemented a phased approach, which is captured in the ISCD Action Plan and includes: documenting all processes and procedures relating to the risk assessment methodology; conducting an internal NPPD review of the risk assessment process; initiating an external peer review of the risk assessment methodology; and engaging national laboratory partners to assist the Department in developing a model for identifying and tiering high-risk chemical facilities based on economic consequences. ISCD has completed the first two phases and in February, ISCD kicked off the third phase with the start of an external peer review. The panel is comprised of nine members with expertise in risk analysis, infrastructure security, toxicology, chemical process safety, chemical weapon analysis, and IED analysis. We expect the peer review to provide input on how DHS can enhance the models including the CFATS tiering model as appropriate. This involves developing an integrated plan with timeframes and milestones that will set the terms for incorporating the results of these activities into an improved risk methodology. While the Department believes that the current external peer review will result in an integrated plan, the Department notes that a second peer review to validate and verify ISCD's risk management approach is worthwhile to consider. NPPD remains committed to both developing appropriate responses to any risk assessment issues that it identifies and keeping Congress and stakeholders apprised of any significant concerns related to that review.

CSAT Tool Suite. As part of its commitment to evolve and mature the CFATS program, ISCD is updating its information technology suite used to collect and process information in the Top-Screen, Security Vulnerability Assessment, and SSP. Refining these CSAT applications will make the overall CFATS process more user-friendly for industry, while making it more efficient

and effective. ISCD has worked with industry to identify focus groups with the purpose of identifying functional requirements for the next generation of the Chemical Security Assessment Tool (CSAT) suite of tools, including the Top-Screen, Security Vulnerability Assessments, and SSPs. In February, the first focus group meeting was held in Texas. Two additional focus groups, scheduled in Pennsylvania and California, will take place in March and April, respectively. The focus groups will engage users of the CSAT Tool to ensure ISCD receives input directly from the regulated community on recommended updates and requirements. Improvements to the CSAT tool suite will provide stakeholders with more advanced technology, improving the process for submitting SSPs and ensuring facilities have a comprehensive picture of risks to their facilities. The public will also have an opportunity to comment on any proposed changes to the CSAT collection tool when it seeks public comment.

Continued Internal Improvements

Over the last year, ISCD has improved many internal operations that address issues identified in the Action Plan. The ISCD Action Plan currently contains 95 items, each of which has been assigned to a member of ISCD's senior leadership team for implementation. The members of the leadership team continue to track established milestones and projected timeframes for the completion of each task assigned to them. In addition, NPPD leadership is deeply engaged with the status of the Action Plan. As of March 5, 2013, 88 of the 95 action items contained in the current Action Plan have been completed. Training, hiring, improving employee morale and ensuring ISCD employees have the appropriate skills are a few examples of some of the internal improvements.

Hiring. ISCD has made significant progress with staffing, including filling several leadership positions. By the end of January, 100% of positions that were vacant on December 1, 2012 have been advertised and ISCD is working to fill the positions with qualified employees. As of March 5, 2013, 22 selections have been made and ISCD expects to have the majority of vacancies selected by the end of March.

ISCD Realignment. Since September 2012, ISCD has successfully realigned its organizational structure to meet the needs of the organization going forward with regard to supervisor to employee ratios both at headquarters and in the field. This includes a realignment of the field operations in order to meet the heightened pace of compliance assistance visits and authorization inspections and the expected commencement of compliance inspections.

Training. From Fall 2011 to Spring 2012, ISCD updated and revised its internal inspections policy and guidance materials for conducting inspections. After releasing the updated guidance materials, ISCD conducted five inspector training sessions, which focused on the updated policy, procedures and related materials to better prepare Chemical Security Inspectors to resume authorization inspections. ISCD has made great strides in improving our inspection process over the past year, and we continue to identify efficiencies to keep moving forward.

One such effort is related to the inspection of RBPS 8–Cyber. Cyber systems are integrated throughout the operations of chemical facilities, including in controlling sensitive processes, granting authorized access, and enabling business. Protecting against cyber attacks on these systems is an essential component in managing overall risk for a facility. In order to further

understand the requirements for the inspection of security measures relating to RBPS 8 and to determine the most efficient path forward, ISCD is in the process of developing a Cyber Security Inspection Standard Operating Procedure and handbook. Additionally, ISCD, in coordination with the NPPD Office of Cybersecurity and Communications, developed training materials for Chemical Inspectors to assist facilities with cyber security integration in their security posture and conducted webinars to better enable each of the inspectors to perform a RBPS 8 inspection at these facilities. In January, ISCD began offering a more extensive training course to allow Inspectors to perform the RBPS 8 inspection for facilities with cyber security integration, which in turn will greatly help the SSP/ASP approval process.

Internal Communications. Throughout NPPD, leadership has promoted staff engagement and a dialogue about issues and concerns through increased leadership updates to employees and a senior leadership open-door policy. ISCD staff has a standing invitation to participate in group open-door sessions or to schedule one-on-one discussions with Division leadership.

Conclusion

We believe the Department has turned a corner on the CFATS program. We are moving forward strategically to address the challenges before us. As we implement CFATS, we will continue to work with stakeholders to get the job done of preventing terrorists from exploiting chemicals or chemical facilities. We firmly believe that CFATS is making the nation more secure by reducing the risks associated with our Nation's chemical infrastructure and we are—along with our stakeholders—committed to its success.

Mr. SHIMKUS. Thank you.

Also joining at the first panel is Mr. David Wulf, who is the director of the Infrastructure Security and Compliance Division. Obviously, you didn't submit an opening statement, nor do you have one, but if you want to have anything just for the record, I would like to recognize you for a few minutes.

STATEMENT OF MR. WULF

Mr. WULF. That would be great. Thank you so much, Chairman Shimkus. I would like to thank you, Ranking Member Tonko, and the other members of the subcommittee for the opportunity to testify here today.

ISCD has made great progress in addressing the challenges described in the internal memo and associated Action Plan that we presented to Under Secretary Beers in the fall of 2011. With strong support from leadership in the National Protection and Programs Directorate and the Office of Infrastructure Protection and through much hard work on the part of the talented men and women of ISCD, we have completed 88 of the 95 items outlined in our Action Plan. We have developed improved policies, procedures, and training to ensure that inspections are conducted in a consistent and thorough fashion. We have implemented an effective streamlined SSP review process, a process that has greatly enhanced our ability to authorize, and as appropriate, grant final approval for Site Security Plans.

We have also done much to stabilize our organization and our leadership cadre by hiring permanent supervisors, including a permanent deputy director, and we continue to foster transparency and open communication throughout our organization.

I would like to recognize our workforce, which truly has a passion for the mission of chemical facility security. And I would like to recognize also the American Federation of Government Employees which represents our bargaining unit employees in the field, and has done much to expedite its review of key policies and procedures over the past several months.

In September I reported that we had turned an important corner in the implementation of CFATS. I am pleased to be able to report today that not only has that corner been turned, but we are moving confidently down the road to realizing the full potential of the program. ISCD and the CFATS program are moving forward in a way that will foster continued advances in the security of America's highest-risk chemical facilities. We have achieved a marked increase in the pace of SSP authorizations, facility inspections, and approved Site Security Plans.

As the Under Secretary noted, we have authorized more than 260 SSPs and granted final approval for 52 of those. We anticipate completing approvals of Site Security Plans for facilities in the highest-risk tier, Tier 1, by September of this year and completing final approvals of Tier 2 SSPs by May of 2014. Reviews and authorizations of Tier 3 SSPs are now underway as well.

However, recognizing that we must find ways to become ever more efficient and effective in our inspection and SSP review processes, we will be looking closely at, and soliciting stakeholder input on, options to streamline the review and approval cycle for facilities

in Tiers 3 and 4. I do anticipate that ASP templates will be an important tool to enhance the efficiency of our reviews. The American Chemistry Council recently worked with us to develop an ASP template and we continue to work with industry associations such as SOCMA, AFPM, and the National Association of Chemical Distributors, who are all considering the adoption of ASP templates for their member companies.

So even as we continue to seek ways to improve, it does bear noting that ISCD's chemical security inspectors are today providing compliance assistance to facilities and conducting inspections at an unprecedented rate. And I am pleased to report that I have received much favorable feedback from our industry stakeholders about their experience with these inspections. As you know, and this is something for which I am profoundly grateful, our stakeholders are not shy when it comes to expressing their candid thoughts and concerns about the program. So I am confident that when I am hearing positive things from industry about their facilities inspections-related experiences, we are on the right track.

I would like to share one quote from Cathi Cross, Director of Security for Phillips 66 regarding a recent inspection in Oklahoma. Ms. Cross conveyed to me that her facility's experience with the DHS inspectors "was a very positive one...that the members of the ISCD inspection team were knowledgeable, courteous, and quite helpful in their collaborative approach as they evaluated the facility, its SSP draft, and planned measures." Continuing, Ms. Cross noted that "the inspectors provided thoughtful comments and were receptive to alternate proposals for meeting security objectives."

So ISCD continues to fully engage with our industry stakeholders, and I very much appreciate industry's continued support for the program. And our stakeholder engagement continues to take many forms. At the facility level, in addition to inspections, we continue to conduct compliance assistance visits and other outreach to work with the facilities as they develop their Site Security Plans. We also engage with stakeholders on important programmatic issues. We continue to work on the development of ASP templates, and we are in the process of gathering industry feedback as we move forward to improve our suite of online tools.

Also, as the Under Secretary noted, we recently concluded a productive and extensive series of discussions on the important issue of personnel surety. Ensuring that those who seek unescorted access to high-risk chemical facilities are vetted for terrorist ties is a critical piece of the CFATS effort and one that we must move forward to implement in the near term.

I am also appreciative of the work done by GAO and the perspectives GAO has offered us on the CFATS risk-tiering methodology and on the management and tracking of our stakeholder outreach activities. With regard to our risk-tiering efforts, while I am confident that our current methodology, with its focus on the consequences of a potential terrorist attack, is appropriate for a regulatory compliance program such as CFATS, considering ways in which our tiering efforts may be enhanced is something to which we are very much open at ISCD.

I am very much eagerly anticipating the results of our external peer review in this regard on risk-tiering and any recommendations that may be forthcoming from the Peer Review Panel.

As for our external outreach, ensuring that we appropriately track and manage our outreach activities is an important priority for ISCD and one that we will pursue.

Thank you again for the opportunity to provide an update on the forward progress the CFATS program continues to make. It is an honor and a privilege to serve with the dedicated professionals at ISCD. I firmly believe we have made much progress in coming together as a regulatory compliance organization, and along with rest of the ISCD team, I am excited and optimistic about the future of the CFATS program.

Thank you again for the opportunity and I welcome any questions that you may have. I apologize for the extra 30 seconds.

Mr. SHIMKUS. Oh, you are fine. Thank you, Mr. Wulf.

And before I recognize myself for the first round of questions, I think just a comment for staff—especially, I think we have some guests in the room—is that maybe we need to put up a placard that defines these acronyms, because if you are visiting this room and you have no idea what these acronyms are, you are like probably listening to Chinese. So stuff like CFATS—Chemical Facility Anti-Terrorism Standards. We will talk about NIPP, which is the National Infrastructure Protection Plan. We will talk about ASP, Alternate Security Plan. So we know there are a lot of you that are well knowledgeable out there, but we probably could do better by having a display of some of these acronyms out there. So I am from the military a long time ago so we were acronym-focused also.

So I will recognize myself for the first 5 minutes of questions and my questions will be directed to Mr. Beers.

Mr. Beers, GAO says CFATS does not consider or analyze vulnerability threat or economic consequence during the tiering process. We knew about the vulnerability gap but not the others. But in GAO's testimony—Government Accounting Office—when would the regulated community, the Hill, and others have learned of this?

Mr. BEERS. Sir, I do not know when the vulnerability issue surfaced specifically, but I do know that it surfaced within at least the last year as far as I am aware. With respect to the economic consequences issue, as I was not present when the program was originally briefed to this committee and other committees, I am simply unaware of when or whether that might have been brought to the Committee's attention.

Mr. SHIMKUS. Yes. So the follow-up is, had not Chairman Upton, Joe Barton, Henry Waxman not asked for this GAO report, we on the Hill and stakeholders may not have learned of the vulnerability gap. Is that safe to say?

Mr. BEERS. Sir, that is certainly a conclusion that can be drawn from that. But one thing that I would add to that, which David and I have both spoken of, is that one of the things that we have asked of the peer review committee after our own internal review is that this methodology be looked at independently. Obviously, we are going to take note of the GAO's comments on this and it is certainly our intention to have full disclosure with you all, and if some of the material is classified, we will do that in a classified setting.

Mr. SHIMKUS. Thank you. According to the National Infrastructure Protection Plan, risk is a function of three components: consequence, threat, and vulnerability—we did this in the last hearing—and a risk assessment approach must assess each one. Have you analyzed the effect of not considering vulnerability for all the regulated facilities?

Mr. BEERS. Sir, we have. The rationale behind that is that while we have——

Mr. SHIMKUS. Did your mike go off or it is not pulled close enough?

Mr. BEERS. Let me start over again. We looked at consequences and threats and gave them a definition in the tiering methodology, but because vulnerability was what the whole program was about reducing and because we did not have the kind of data that we needed in order to be able to assign vulnerability factors with specific and differentiated levels, we chose to hold that constant, tier on the basis of threat and consequence, and ask the facilities then to come back to us with an indication of what their vulnerabilities were and to work with them on Site Security Plans to deal with those vulnerabilities.

The consequence of this is that the tiering works to set them aside by threat and vulnerability and the whole endgame is about reducing vulnerability or risk. So we chose to hold that constant in the tiering; we chose to deal with that through the Site Security Plan process.

Mr. SHIMKUS. And I guess then our follow-up would be we think you have evaluated part of the threat, not the entire threat, and there is no economic process that has been defined so far which is a part of that whole calculation. But you did identify in your comment about up-to-date data. So what is the effect of not using up-to-date threat data in the risk-tiering approach?

Mr. BEERS. Sir, as we go through this process, if there is additional threat data or altered threat data, our intention is to include that. That is certainly something that we are talking with the Peer Review Committee about and my guess is we will get some different information.

David, do you want to add to that?

Mr. WULF. Yes, I would. Yes, the tiering methodology, as it currently exists, is certainly very much consequence-based. I think that consequence is tied very much directly to threat as we use the threat in the tiering engine. Targets that have high value from a terrorist perspective in terms of the consequence will also typically have a pretty high score on the threat side. We are certainly very much open to ways in which we can enhance the tiering methodology and that is the very reason we are having this external peer review.

But I think focusing principally on consequence in a regulatory compliance framework is an appropriate way to tier facilities. If we focused heavily on vulnerability in the actual tiering, we would have potential situations in which a facility would tier highly because of a heightened vulnerability that it identified. As a result of tiering highly, it would put into place hopefully significant and successful security measures to address the vulnerability. The vulnerability would then be diminished and theoretically that facility

would tier out, not have those requirements any longer, conceivably have its vulnerability go up again, tier back in, and we would have sort of a roller coaster effect.

So I think the way in which we and the CFATS program have woven the vulnerability factor into the remainder of the program in the facilities, assessment of vulnerabilities, in the development of their security vulnerability assessments, and in their development of Site Security Plans makes sense. That is not to say there isn't room for improvement and I certainly anticipate we will get some solid recommendations in those regards from the Peer Review Panel.

Mr. SHIMKUS. Thank you. My time has expired. The chair now recognizes Mr. Tonko for 5 minutes.

Mr. TONKO. Thank you, Mr. Chair.

It appears that the Department of Homeland Security has good progress to report implementing their Action Plan to strengthen the CFATS program, but I am concerned that fundamental problems may still exist. I would like to focus on one of those concerns and that has just been the focus of the chair's address and that being the tiering of facilities.

CFATS is a risk-based program meaning that facilities placed in a high-risk tier have to meet higher standards, I am told, for security. Lower-tiered facilities then meet lower standards. An error in tiering could mean that a high-risk facility is not adequately secured or that the owners and operators of a low-risk facility have to invest in unnecessary security measures. The tiering process must be, therefore, as accurate as possible.

The Department published a National Infrastructure Protection Plan in 2006 and I believe revised it in 2009. This plan discusses how risk analysis for terrorism threats should be conducted. Under Secretary Beers, should the CFATS program be consistent with that plan, the developed plan of 2006, and improved in '09?

Mr. BEERS. Sir, the National Infrastructure and Protection Plan is a global statement of risk. All of the programs in the Department of Homeland Security should be in rough alignment with that. But we also have to recognize that different sectors and different companies may have some specifics that cause some alteration or some specific requirement relevant to them and perhaps only to them. But as a general measure, yes, that is correct, sir.

Mr. TONKO. So as a general measure, we say yes. And according to the National Infrastructure Protection Plan, risk assessments must account for threat, vulnerability, and consequences. But that is not what CFATS, as a program, currently does. GAO is critical of the fact that apparently DHS completely ignores the potential economic consequences of a terrorist attack when conducting a risk assessment. And GAO is not the first to say this. In 2010, the National Academies published a report, requested by Congress, on department-wide efforts to analyze risk. And the Academies approved of the framework in the National Infrastructure Protection Plan but found that "many of the Department's risk-analysis models and processes are weak and are not on a trajectory to improve." According to Academies, the methods were not "documented, reproducible, transparent, or defensible."

These are very serious criticisms and to address these issues the National Academies made a number of specific recommendations. So my question to you, Under Secretary, is that did the Department ever provide a formal response to the National Academies' report?

Mr. BEERS. Sir, there was a response by the Department to that. I can get you a copy of that. I don't have it on hand at this particular point in time. But we were certainly aware of the Academies' report and we did respond to it.

Mr. TONKO. Under Secretary Beers, can you please explain the process you are currently engaged in to improve the risk assessment done in the CFATS program and whether it will respond to the recommendations made by GAO and the National Academies?

Mr. BEERS. Sir, let me respond on two levels here, first, to go back to the original premise, which is the threat, consequences, and vulnerability address how one should be dealing with risk and simply say we believe in the CFATS program that we do address all three of those aspects even though the tiering methodology, which is not the entire dealing with risk, only focuses on consequences and threat and holds vulnerability constant. But as I said in my earlier response to the chairman's question, we believe that the vulnerability part of that equation is dealt with in the development of the Site Security Plans.

With respect to the larger question, I think that what we are trying to do here is work through a regulatory program which is different—the NIPP was really written in association with voluntary programs, which meant that while we could lay out best practices or standards or thoughts on how to deal with this, it was really entirely up to the companies in order to do that. And in the regulatory program, we have the ability to state whether or not their response is in fact adequate to the regulatory requirement that we have. And that makes it somewhat different from the framework in which the NIPP was written.

But let me also turned to David Wulf to add anything that he may wish to add.

Mr. WULF. I would just add a couple of things. We committed to do three things when we encountered some issues with the tiering methodology. One was to do an internal documentation of our processes and our methodology, do sort of an internal department look at the CFATS methodology and to do what is ongoing right now, the external peer review. As we conducted our documentation, we have tried to be transparent about what we found. We have talked through issues with staff up here, with our industry stakeholders, and have tried to keep everyone abreast of the progress we are making on the economic criticality piece of this, of the consequence assessment in the tiering methodology.

In that regard, I would note for the Committee that we are actively engaged in trying to address the economic consequence part of the equation. We are working with Sandia National Labs on that effort. I received a briefing I want to say a couple of months ago. Our expectation is that Sandia's work—and it is difficult stuff assessing economic consequences of potential terrorist attack—will be complete in early 2014. We anticipate talking through the Sandia findings with our stakeholders. We are not going to proceed in a

vacuum as we look to incorporate economic consequence into the model, but I do believe, as I think you do as well, that it is an important piece to the puzzle. So we are going to continue to seek to improve the methodology.

The thing we struggle with is trying to be a continually improving program, at the same time trying to afford a degree of certainty to our industry stakeholders for whom it would be difficult to have an ever-changing target in terms of the tiering. So we have to balance all of that, but we are taking a hard look at it all.

Mr. TONKO. Thank you.

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

Again the NIPP is the National Infrastructure Protection Plan again for our guests who are now leaving.

So the chair now recognizes the gentleman from Pennsylvania, Mr. Pitts, for 5 minutes.

Mr. PITTS. Thank you, Mr. Chairman. Under Secretary Beers, according to the NIPP, risk management should help focus planning and allocate resources. How can you prioritize resources and manage risk if you don't differentiate between threat or vulnerability?

Mr. BEERS. Sir, we definitely do differentiate between threat and vulnerability. What we have tried to do here is ensure that the compliance part of the effort which is to buy down risk, it was measured against the threat-and-consequence tiering of the tiering methodology. So the whole program is designed to reduce the vulnerability to the American people, to the communities that surround those facilities. And every effort is made through the risk-based performance standards to help those facilities produce Site Security Plans that in fact protect the communities in which they live far more than when there was no regulation on those facilities. Which is not to say that they weren't trying in their own way to do that, but what we have tried to do is to provide a general way in which they can approach that to help them or to give them thoughts about other ways that they might think about buying down that risk by reducing the vulnerabilities through their Site Security Plans.

David, would you add anything?

Mr. WULF. No. I think that pretty well covers it. The vulnerability is, as I have expressed, woven through the fabric of the program in the security vulnerability assessments that facilities conduct, and in their development of Site Security Plans.

Mr. PITTS. Given incomplete aspects of your risk assessment model, are you confident that the CFATS risk-tiering approach adequately tiers facilities?

Mr. BEERS. Based on the way that we have put forward the methodology, we are confident that the general model is correct, as has been indicated here. We are going to look at economic consequences to see whether or not—and if so, how—that ought to be injected into the methodology. And we are reviewing the threat information as well. So this, as David just said, is not a static program and we are looking for assistance and help from the peer review effort to see how we might do a better job. But as David also said, we want to do this in a fashion in which we are not constantly changing and moving everything because industry also

needs a degree of stability as they consider how to improve their own site security.

Mr. PITTS. Now why do you collect data, information that you do not use? Regulated facilities are required to provide substantial information to facilitate the tiering process but ISCD only uses a small amount of this data.

Mr. WULF. My assessment is that all of the data that we take in is valuable to the program, and it is useful as we evaluate, not only the tiering as we assign risk tiers but as we look at evaluation of Site Security Plans. So the questions and the information that is provided in response to those questions I think goes a long way toward prompting facilities to give thought to their vulnerabilities and to incorporate appropriate responses to those vulnerabilities and to implement security measures appropriate to respond to those vulnerabilities as they develop their Site Security Plans.

Mr. PITTS. My time has expired. Thank you.

Mr. SHIMKUS. The gentleman's time has expired. I would hope that he will pay close attention to the GAO report because they say, obviously, there is a lot of data that is not used and that is the reason why that question is asked.

Five minutes to Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman.

Welcome to our panel. Under Secretary Beers, in your testimony for today's hearing you state that DHS will be publishing a revised Personnel Surety Program rule next week. Regarding the PSP, are you able to commit today that the new rule will allow similar credential programs like the TWIC program for land-based—so we would have one ID for employees whether they work for a company's land-based site or the water-based site?

Mr. BEERS. Sir, you are correct. We have provided our Personnel Surety Program notice to the Federal Register and the Department has provided a TWIC Reader Rule Requirement Program to the Federal Register also this week. Those will be published, I am told, next week. It takes that long to actually put it out. It will include the ability to use a TWIC card as a personnel identification and personnel surety credential within the program for those who qualify for the program. The larger TWIC reader rule will allow companies, facilities to know what kind of a validation system they have in order for those TWIC cards to be validated as individuals pass into those facilities. That was, as you will recall, an original requirement of the whole TWIC program, which has been operating unfortunately without that reader rule requirement up to this point in time.

Mr. GREEN. Well, and we have talked about this for a couple of years now and I appreciate the agencies doing that because a lot of plants have waterside and land-based—and employees move back and forth and most of the time the employees have to buy those cards themselves and it just seems like it did not make any sense to make an employee, you know, have to buy two cards that really should be issued by the Federal Government. You only need one.

Mr. BEERS. I couldn't agree with you more, sir.

Mr. GREEN. And can you share the efforts the Department made to incorporate both employee and union interest, because I know of

some in my area—we have steelworkers that represent my refiners and chemical plants, a number of them. Were they involved in this decision or received input?

Mr. WULF. The earlier information collection request that was withdrawn during the summer was open for comment across the board. We did not work specifically or discuss any of this specifically with labor unions.

Mr. GREEN. OK. Well, I know one of their concerns is that their members would have to have these two cards. And when does your agency anticipate to complete the site security program review for all facilities and including Tier 3 and 4?

Mr. WULF. As I mentioned, we are looking to be through with Tiers 1 and 2 by the first part of 2014. With regard to Tiers 3 and 4, we are looking at ways that we can increase the pace of the review. I know the GAO, looking at sort of the current pace, has projected it could take between 6 to 9 years. That is a pace that is, in our view, not an acceptable one. I think that we are going to continue to see the pace quicken. I don't want to provide a certain date because I am sure I will be slightly off.

But I think as we move forward with the heightened pace of inspections as we learn more about how to achieve efficiencies in the SSP reviews and the inspection process, we will get better at doing them and be able to inspect, review, and approve larger numbers of SSPs. I think the alternative security programs will provide a means to heighten the pace as well. So as those templates come into greater use, and particularly as they are used by multiple facilities within the same company, I think we will see the pace quicken significantly. We will also continue to look at the resources we have to do those inspections. We are bringing on board another 18 inspectors which will increase our capacity. We will continue to look at whether there might be a possibility of getting some additional folks on board as well.

Mr. GREEN. Mr. Chairman, I know my time is—but there has been a substantial public sector investment and private sector investment and we would hope to see some of that, that they would have their security plans at least on what they have invested literally hundreds of millions of dollars on, both, like I said, public money and private money.

Thank you, Mr. Chairman.

Mr. SHIMKUS. The gentleman's time has expired. Before I move to Mr. Cassidy, just for clarification, Mr. Wulf, and for the transcriber, when you said the 6 to 9 years did you say is not an acceptable or did you say not unacceptable?

Mr. WULF. I said it is not acceptable.

Mr. SHIMKUS. OK.

Mr. WULF. It is not an acceptable——

Mr. SHIMKUS. Great. Thank you. It caught my attention there for a second.

So now the chair recognizes the gentleman from Louisiana, Mr. Cassidy, for 5 minutes.

Mr. CASSIDY. Hey, gentlemen. Thank you for being here. I understand that you all have done a heck of a lot of work to address some of the issues and as I have obviously been a sharp critic, so first, I thank you for your hard work that you have done.

With that said, you might guess I have got a couple other concerns. The fact that you can——

Mr. WULF. I said I suspected you might.

Mr. CASSIDY. The fact that you can buy down risk or buy down vulnerability by decreasing threat suggests that risk is some constant. You have some number for risk, however you calculate that number, that you would like to address. It is also my understanding, I think you said earlier, the review panel will come up with a new model in which they will assess both the economic consequences and life consequences and all these other factors in a more sophisticated fashion than currently you are doing. Are they going to have access to your data—this category of data, this continuum of data that you have—in order to see the robustness of their model?

Mr. WULF. Yes, sir. The Peer Review Panel has access to everything that we have, classified and otherwise.

Mr. CASSIDY. Now, is it possible that that will show that what you are currently doing is—I suppose that means if they are coming up with a new model, it will show either that you are doing a good job or that you are not doing a good job. Correct?

Mr. WULF. Well, I don't know that it is fair to say that the panel's charter is to come up with a new model. The charter is to take a fresh look at what we are doing.

Mr. CASSIDY. But if you don't currently have—I don't mean to interrupt, I am sorry. It is limited time. If you don't have economic consequences in there, and I understand at some point, reading the testimony or GAO report, that population density wasn't factored in some places. It certainly seems that you need a new model. Does that make sense? I mean if we are going to include economic consequences, and what you are doing now does not do so, then clearly you need new model.

Mr. WULF. As we look to incorporate economic consequences—and I should mention that at Sandia National Labs that is doing the work for us on economic consequences—but certainly something the Peer Review Panel can, and I suspect will, look at as well. As we move to incorporate that into the model certainly we would have to revise the model.

Mr. CASSIDY. So you do anticipate giving them access to your compendium of information for them to check to see the robustness of the model?

Mr. WULF. Absolutely.

Mr. CASSIDY. And will you share that with the Committee?

Mr. WULF. We can certainly look at that——

Mr. CASSIDY. I mean, like, why wouldn't you?

Mr. WULF. I don't see why not.

Mr. CASSIDY. Yes. Now, if you decide upon this model as being that model which you should use, would you share it with the industry?

Mr. WULF. The underlying information?

Mr. CASSIDY. No, not the underlying information, the model itself. Because if, Mr. Beers, you say that they can buy down vulnerability by whatever—addressing in a greater way threat—I imagine you have some retrogression analysis and that you can

plug these things in. Really, right now, it appears that there is a certain degree of subjectivity.

Mr. WULF. Well, looking——

Mr. BEERS. Sir, we are committed. And that is one of the questions that we have asked the peer review to look at is, what should we share from the tiering methodology with them? Now, we have some parts of it which are currently classified. We are also looking at the possibility of declassifying some of that information as well. Because we firmly believe as the program has matured that the transparency of the tiering model is important. That will help them think about their own Site Security Plans in a better way than to simply use the risk-based performance standards by themselves. The objective here is to reduce risk. The objective here is to reduce vulnerability and we believe as we have considered this, that that kind of transparency is necessary.

If there remains classified parts of the program, we will look at whether or not we can at least have some industry representatives, as we do generally with the National Infrastructure Protection Plan, cleared to receive classified information even if we can't make it broadly available.

Mr. CASSIDY. So I am asking now, not to challenge but rather for information, if you have a formula by which someone can decide what their relative risk is, you plug in these variables and you come up risk, it seems to me that—I don't know whether that would be classified. Listen, a 15-foot fence will get you here and a 30-foot fence will get you there and video cameras will get you here and armored cars will get you there. So knowing that some of the information is classified, are the variables that you plug in classified?

Mr. BEERS. David?

Mr. WULF. Some of the factors that go into the calculation of the risk score are classified. But I would just echo the Under Secretary's comments that fostering greater transparency for our stakeholders in tiering is one of our goals and certainly one that we are going to pursue.

Mr. CASSIDY. Last question—and you may have mentioned this earlier—when do you expect the panel to come back with their report and then ideally to run some of those compendium of information to check out what you have been currently doing and et cetera?

Mr. WULF. We are anticipating a report from the Peer Review Panel this summer.

Mr. CASSIDY. OK. Thank you. I yield back.

Mr. SHIMKUS. The gentleman yields back his time. The chair now recognizes the ranking member of the full committee, Mr. Waxman, for 5 minutes.

Mr. WAXMAN. Thank you, Mr. Chairman. Today's hearing underscores the need for reform of this program, and in my view, this committee should develop comprehensive reauthorization legislation.

Today, GAO will testify that it will take 8 to 10 years before the Department can review and approve the Site Security Plans it has already received. Additionally, the Department must revise its risk analysis model, which could mean that the current tiering of facili-

ties will have to be revised, requiring many facilities to begin the process over again.

In the 111th Congress, the Committee produced a comprehensive Chemical and Water Facility Security Bill to finally set this program on the path to sustainable success. Mr. Beers, you testified in support of that bill as did representatives of the labor community, the environmental community, water utilities, and the chemical industry. At that time you said, "given the complexity of chemical facility regulation, the Department is committed to fully exploring all issues before the program is made permanent." I agree with that statement and I would like to explore some of those issues with you today.

Mr. Beers, does the administration still support closing security gaps for wastewater and drinking water facilities?

Mr. BEERS. Yes, sir.

Mr. WAXMAN. Does the administration still support maintaining EPA as the lead agency for drinking water and wastewater facilities with the Department supporting EPA's efforts?

Mr. BEERS. That is our position.

Mr. WAXMAN. Does the administration still believe that all high-risk chemical facilities should assess inherently safer technology and that the appropriate regulatory entity should have the authority to require the highest-risk facilities to implement those inherently safer technologies if feasible?

Mr. BEERS. The statement at that time still remains the administration's position, sir.

Mr. WAXMAN. Since we worked on that bill 3 years ago, additional challenges have come to light. Specifically, the internal review and memorandum prepared in November 2011 found serious problems. The Department produced an Action Plan to address these problems. That Action Plan included the formation of a task force to develop recommendations for legislative and regulatory changes to the CFATS program. My understanding is that the Department reports that it has completed development of those recommendations. Mr. Beers, when can we expect to see those recommendations?

Mr. BEERS. Sir, I will have to get back to you on that. I don't have specific answer on that question.

Mr. WAXMAN. OK. Well, I look forward to you getting back and to have the record held open so that we can get that response.

Mr. SHIMKUS. Without objection. So ordered.

Mr. WAXMAN. As the Committee further considers the CFATS program, having your legislative recommendations for reforming the program would obviously be very helpful.

Thank you, Mr. Chairman. I yield back my time.

Mr. SHIMKUS. The gentleman yields back his time. The chair now recognizes the other gentleman from Pennsylvania, Mr. Murphy, for 5 minutes.

Mr. MURPHY. Thank you, Mr. Chairman. And thank you, to the panel.

According to the CFATS rule, a high-risk chemical facility is one that, in the discretion of the Under Secretary, presents a high risk of significant consequences for human life and health and now security and critical assets. Let me ask you a few comments on this.

If, as a result of your work with Sandia National Laboratories economic consequences are incorporated into the CFATS risk-tiering approach, how will this impact the current list of related facilities and do you expect more facilities to be covered?

Mr. WULF. I think it is hard to say right now. Depending on what we get back and our analysis of Sandia's work, it could impact the number of facilities that are covered in a few different ways. Depending on the weighting that is given to the economic consequence piece of the equation and really the general fabric of the assessment on economic consequences. So I don't think I am in a position today to forecast that.

Mr. MURPHY. Can you give any estimates at all how much you think it is going to cost to incorporate the results of the Sandia National Laboratories work into the current CFATS risk assessment approach?

Mr. WULF. I don't at this time, not without the assessment from Sandia.

Mr. MURPHY. Well, given also it is going take approximately 7 to 9 years for ISCD to review plans submitted by regular facilities, how practical is it for you to expand the program to include additional facilities?

Mr. WULF. We are going to, first, as I said, the 6 to 9 years is not an acceptable pace and we are going to do everything in our power to pick up that pace. I think though that it is important that we foster enhanced security for all chemical facilities that are high risk in nature. So, to the extent the universe of high-risk facilities is framed and includes in the calculation of that universe or in the formation of that universe the economic consequences and the universe grows, we will look at ways to make that work.

As I said, we are bringing on additional inspectors; we are improving our processes and procedures. We are going to get better and better at this. So, if that challenge presents itself, we will meet the challenge.

Mr. MURPHY. I know we have talked about these things in other hearings that the chairman has conducted here, and you are expecting about 30 to 40 site plan approvals per month. That is your anticipated goal for the future?

Mr. WULF. That is our current pace.

Mr. MURPHY. The current pace. Well, how may did you approve in January of 2013?

Mr. WULF. I would have to get that to you specifically.

Mr. MURPHY. February? Just last month, any idea?

Mr. WULF. I would imagine between 20 and 30 in February.

Mr. MURPHY. So you said you expect——

Mr. WULF. Yes.

Mr. MURPHY. You are currently at 30 to 40 but you are half that in February. I am just trying to——

Mr. WULF. Yes. I expect it is going to continue to ramp up because what we are doing more of in January and February was authorizing plans. And as we authorize the plans, we schedule the inspections. That is what leads to the approvals. So the approval pace will pick up. We anticipate by the end of September being up to upwards of 350 approvals. So that will be all of Tier 1 and probably about halfway through the Tier 2 facilities. So, actually, in 6

months, 6½ months from now, we will likely be doing about 50 approvals a month for the next foreseeable future.

Mr. MURPHY. You have a mechanism for continuous improvement as you go through these to speed them up, for example, getting feedback as you go through these approval processes—feedback from people you have worked on with those saying what we could have done to make this better, faster, more thorough?

Mr. WULF. Yes, we sure do. We are constantly evaluating our processes and looking at ways we can do things better.

Mr. MURPHY. Is that an internal process? Do you also get external feedback on that?

Mr. WULF. Well, it is an internal certainly within the division and the relevant branches within the division. But also we are talking consistently with our stakeholders, and I was able to share one comment we received back during my opening statement. But we are always talking to our stakeholders about improving. And one of the things we have done to pick up the pace and to increase the pace of SSP authorizations and approvals specifically has been to include our field inspectors, who are most familiar with the facilities in the authorization and approval loop early in the processes. As issues are identified, those SSPs are kicked out to the field and squared away and kicked back into the authorization and approval loop more quickly.

Mr. MURPHY. In my remaining time I just want to ask real quick. We understand there are some documentation issues regarding the CFATS risk-tiering approach. Can you give me a little information of what those documentation issues are? Is that something slowing you down, too, or what are those documentation issues?

Mr. WULF. No, I don't think so. The documentation I referenced earlier was our effort over the past year to thoroughly document the tiering methodology.

Mr. MURPHY. Is that also improving over time? Thoroughly documenting so you are——

Mr. WULF. Yes.

Mr. MURPHY. Well, I am out of time here I know but I will follow up on the other questions. Thank you.

Mr. WULF. OK.

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

The chair now recognizes the gentleman from California, Mr. McNerney, for 5 minutes.

Mr. MCNERNEY. Thank you, Mr. Chairman.

Mr. Wulf, is the ISCD responsible for addressing cyber threats to chemical plants?

Mr. WULF. Yes, sir. Yes, sir. One of our Risk-Based Performance Standards, RBPS 8, relates to cyber.

Mr. MCNERNEY. So are there specific cyber threats for potential catastrophic results to human beings that you know of?

Mr. WULF. I think potentially there could be, which is why CFATS addresses cyber. It focuses within the CFATS framework on industrial control systems, on systems that can impact the release of chemicals, and on systems that can impact the security of a facility.

Mr. MCNERNEY. So how effective then is the DHS in addressing these potential cyber threats?

Mr. BEERS. Sir, we have the best team in the country to deal with industrial control systems as announced by Security magazine. The ICS or Industrial Control Systems team that we have in our cyber office is absolutely the best in the country. They provide regular assessments on requests from people. We are expanding that program. It will also be part of the work that we are doing with respect to the Executive Order on cybersecurity and the Presidential Policy Directive that came out, both for those in February, a major area of concern and a major area of involvement. We are basically teaching the rest of the government how to deal with this issue.

Mr. MCNERNEY. Good. Good. In my mind there are two aspects of cyber defense: protection and retaliation. Maybe that is not the way that you look at it, but a kinetic attack will almost certainly involve a strong response from this government. But on the other hand, a cyber attack may not elicit a response. So the question I have is, are there rules of engagement for cyber attacks on chemical facilities in this country?

Mr. BEERS. Sir, there are general rules of engagement that is not part of the DHS activity set. That belongs to the Department of Defense. But we and the Department of Defense and the Department of Justice have a very robust effort to work together on a regular basis at all of those things short of an actual attack. I mean, we are, as you well know, in a sort of cold state of a lot of reconnaissance, a lot of intellectual property theft that is going on now that the three departments are working mightily to try to deal with. But the offensive side is the domain of the Department of Defense. We are aware of what they do in a general sense but it is not part of our responsibility.

Mr. MCNERNEY. So I mean there must be some coordination then. I mean cyber attacks are happening on a continuing basis, some of them less of a threat and some of them more of a threat. And so what I would like to get is some comfort that there is going to be a consequence to conducting cyber attacks at any level on facilities in this country.

Mr. BEERS. Sir, I certainly can't comment on that in this unclassified setting.

Mr. MCNERNEY. OK. Mr. Chairman, I yield back.

Mr. SHIMKUS. The gentleman yields back the time.

The chair now recognizes the gentleman from West Virginia, Mr. McKinley, for 5 minutes.

Mr. MCKINLEY. Thank you, Mr. Chairman. This is an interesting subject.

Mr. SHIMKUS. Mr. McKinley, can you turn your mike on, I think?

Mr. MCKINLEY. It is on.

Mr. SHIMKUS. Oh, you do.

Mr. MCKINLEY. Yes, this is an interesting subject. As an engineer and as someone who has worked in some of these chemical plants, I am curious to learn more about what we have been doing and how long it has been going on. I am just curious, first, I guess is, do either of you feel are terrorism threats on the rise? Is it status? What is happening in this country? I am just curious.

Mr. BEERS. Yes, sir. That is a very good question. I think what we have seen since 9/11, a continued threat within the country that

has been primarily executed by individuals who have been inspired by the rhetoric of the jihadists to conduct acts within the country. Fortunately, we have been able to thwart most of them. Some of them just simply failed because they weren't very well executed. The Bureau has a very extensive program trying to detect this. Could something happen from overseas again? Yes, that is always a possibility, but that is a major effort that we and the other departments are working on.

Mr. MCKINLEY. Well, again, are the attacks on the rise? Threats I should say. Are threats of attacks on the rise?

Mr. BEERS. Are threats of attacks on the rise? The threat and capability, because aspirational threats——

Mr. MCKINLEY. It should be just a yes or no. Isn't it a yes or no?

Mr. BEERS [continuing]. Occur on a regular basis and you could look—and there is something every day. Threat and capability matched with one another——

Mr. MCKINLEY. Are threats on the rise?

Mr. BEERS [continuing]. I think at this point are not on the rise.

Mr. MCKINLEY. OK. That is fine.

Mr. BEERS. Are not on the rise.

Mr. MCKINLEY. What is their objective? Is it just to have access? Are they trying to just blow up a facility? What is the threat that you are hearing? What are they trying to accomplish?

Mr. BEERS. So there is the local objective and there is the broader objective, and they think in both of these realms. The local objective is to have an event that is sufficiently newsworthy, sufficiently damaging, that it causes people to take notice of it and gives them credit for the ability to actually execute. The broader issue, though, is to destroy—and bin Laden and his successors have been very clear about this—is to destroy the will of the West, and the will of the United States to oppose them and withdraw from the region.

Mr. MCKINLEY. So if I can continue with the question, can you give me an example of a chemical facility that has been attacked successfully in the West?

Mr. BEERS. No, sir. Unless you want to include the Amenas plant in Algeria, which is the one recent one——

Mr. MCKINLEY. OK. That is fair.

Mr. BEERS [continuing]. That we had, but other than that, I can't tell you.

Mr. MCKINLEY. It is one thing if they want to disrupt it, would we not pose a threat also in where the products that we are producing in these chemical plants—does it extend your risk assessment and evaluation? Does that also go to the distribution centers and transportation or is it just at the plant?

Mr. BEERS. It is in all of those, sir, depending upon the holdings, where the holdings are——

Mr. MCKINLEY. So you go the whole route. You are not just on risk assessment——

Mr. BEERS. But again, if the holding isn't large enough to be tiered in by the consequence, then they are not regulated. But we do look at distribution centers as well. David, you want to——

Mr. WULF. But CFATS focuses on facilities. So there are other agencies that deal with the transportation sectors. So the transportation of hazardous materials is covered by the Department of

Transportation and the Transportation Security Administration. CFATS is focused on facilities but certainly including distribution centers. And among the chemicals of interest that we assess are those chemicals that could be successfully used by terrorists in an attack as well as chemicals that can be released.

Mr. MCKINLEY. In the time frame that I have left, are the four other European nations, do they have something comparable to what we are doing here?

Mr. WULF. I think in many ways we are on the cutting edge here. And I think CFATS is a sound program and really a model that, were it implemented elsewhere could be of value to securing chemical facilities and hardening them against potential terrorist attacks.

Mr. SHIMKUS. Gentleman's——

Mr. MCKINLEY. OK. Time has expired on that, but I just want to say, even though they have not had an attack in Europe and they don't have anything comparable to this, I am just curious.

Mr. WULF. I think Congress' assessment and our assessment as well is that high-risk chemical facilities pose a very attractive target to terrorists.

Mr. MCKINLEY. Thank you.

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

The chair will now recognize the gentleman from Ohio, Mr. Johnson, for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. Beers, the Department of Homeland Security has adjusted its chemicals-of-interest release model because of errors in the formula. Are you aware of any other issues that may affect this or any other models within the risk assessment approach?

Mr. BEERS. Sir, I am not, but let me turn to my expert here and ask him if there is anything you want to add to that.

Mr. WULF. No. Our documentation found some minor issues that we have briefed staff on and that we have addressed and that have not led to significant re-tierings or significant numbers of re-tierings of facilities. So we are looking forward to receiving the report from the Peer Review Panel and any recommendations for improvements they may have for the tiering engine.

Mr. JOHNSON. Is this the expert panel review that you are talking about?

Mr. WULF. That is right.

Mr. JOHNSON. OK. Before you became aware of problems with the chemicals-of-interest release model, had you conducted any evaluations, Mr. Beers, of the risk-tiering approach?

Mr. BEERS. Sir, before we became aware of that particular problem, I am not aware of any reviews that had taken place. Having said that, it was, as we look backward on when that matter was brought to my attention, that there were questions about it a year prior to that. And the review that happened at that time turned out not to be an accurate review. So in that sense, there were anomalies that were looked at; unfortunately, they failed to detect the problem that ultimately surfaced several years ago.

Mr. JOHNSON. OK. All right. In regards to the expert panel review, it is our understanding that the current expert panel review

will not include a formal validation or verification of the model. How does that impact the value of the review?

Mr. WULF. We have asked the panel to take a full look at the program, at the tiering methodology, and to give us an assessment as to whether it is, in fact, a sound methodology for assessing risk and also to provide us any recommendations for potential enhancements and improvements to the methodology. So I don't anticipate a formal stamp of approval, but I expect that they will let us know how they feel about what we are doing in the tiering arena.

Mr. JOHNSON. But it is important though, right? I mean, it is important to get that information, to get that stamp of approval.

Mr. WULF. I think that is why we are doing this. Not to——

Mr. JOHNSON. But you said you are not expecting a stamp of approval.

Mr. WULF. Well, not——

Mr. JOHNSON. So there is——

Mr. WULF [continuing]. An actual stamp, I guess.

Mr. JOHNSON. Yes.

Mr. WULF. I am——

Mr. JOHNSON. We don't want them to just look at it; we want them to give us a validation and verification that the model is accurate according to what we know today. Correct?

Mr. WULF. Yes. We want them to look at the methodology and let us know their thoughts on whether it works and if there are ways in which it could work better.

Mr. JOHNSON. OK. Given that you have not been able to review the Site Security Plans for the Tier 3 and 4 facilities, how would you characterize how they are currently being regulated?

Mr. WULF. Well, I would mention that we have begun review of the Tier 3 Site Security Plans and I have authorized some of those. But that is admittedly in the early stages.

Mr. JOHNSON. Tier 3 and 4, or just 3?

Mr. WULF. Tier 3. Tier 3.

Mr. JOHNSON. OK. So 4 is not being included?

Mr. WULF. Tier 4 reviews have not begun on the SSPs. But I would say that across the tiers to include Tiers 3 and 4 CFATS has had an impact. Those Tier 3 and Tier 4 facilities have gone through the top screen process, have developed security vulnerability assessments, have, in most cases, met directly with CFATS inspectors who have worked with them through compliance assistance visits and other outreach in the order of more than 3,000 such visits and encounters to work with them on the development of their Site Security Plans. So I think in all cases, even without authorization or approval of those facilities, their security has been enhanced by CFATS and the work of our inspectors.

Mr. JOHNSON. OK. With that I yield back, Mr. Chairman.

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

The chair now recognizes the gentleman from Mississippi, Mr. Harper, for 5 minutes.

Mr. HARPER. Thank you, Mr. Chairman.

Thank you, gentlemen for being here. I know this is always an exciting time, but we welcome you and appreciate the insight. We are obviously concerned about security for these facilities, how we accomplish that. And as we are looking at the number of facilities

we have, has there ever been any thought on your side of maybe just limiting the scope of regulating facilities only to the Tier 1 and Tier 2 facilities? Has there been any thought on that?

Mr. WULF. I would say that, no, there hasn't. Inasmuch as all four tiers represent high-risk chemical facilities and a relatively small percentage of the total number of chemical facilities in the country, our assessment is that all four tiers are worth covering under CFATS.

Mr. HARPER. Do you agree with that?

Mr. BEERS. Sir, remembering that this is a consequence-focused——

Mr. HARPER. Yes, sir.

Mr. BEERS [continuing]. Issue, the original decision on all four of the tiers were that the consequences, the potential loss of life in the vicinity of those facilities—this is the primary reason——

Mr. HARPER. Yes, sir.

Mr. BEERS [continuing]. Was significant in terms of the communities that surrounded them. So it is, as you well know, impossible to put a cost on the loss of even one life. So that is why this is such an important decision and why we really haven't gone that step and said, no, that 3 and 4 are not high-risk.

Mr. HARPER. OK. Let me ask this: as you are establishing these, you do a preliminary tier risk rating and then you do further evaluation—the SVA—and you determine what the final rating is.

Mr. BEERS. Yes.

Mr. HARPER. And once that is established, what is the review process after that? Is there a time with that final tier risk rating that it might change in the future? How often are you going back to review those?

Mr. WULF. As facilities make changes to their chemical holdings or to their processes, they may submit a request for redetermination or may submit a revised top screen to ISCD and we will, you know, rerun that and assign as appropriate a——

Mr. BEERS. So the nearly 3,000 changes that have been made——

Mr. HARPER. Sure.

Mr. BEERS [continuing]. Including tiering out are a result of changes in holdings that have been able——

Mr. HARPER. OK.

Mr. BEERS [continuing]. To be recognized in that fashion.

Mr. HARPER. So is that possible review or change of a tier risk, is that something that you have to wait on them to notify you or are you on a schedule? Do you go back and review those yourself even if you are not notified of any changes on their part?

Mr. WULF. To the extent that our inspectors are out working with these facilities through compliance assistance visits or other outreach——

Mr. HARPER. OK.

Mr. WULF [continuing]. That is sort of the form that would take. So our involvement would happen in that way but there is not a formal process for going back and——

Mr. HARPER. Not a calendar date say every 2 years, 3 years we are going to come back and review? OK. Now, it is my understanding that if you have two facilities that have the same chem-

ical of interest, one that has very little physical security near a major city, and another stored with the same chemical in an extremely secure location near that same major city, they would be tiered identically? Is that accurate? If it is the same chemical of interest, regardless of the level of security near that major city, in two different facilities, would they be tiered the same?

Mr. WULF. I think that is accurate.

Mr. HARPER. OK.

Mr. WULF. The tiering is based on the potential consequence of that.

Mr. HARPER. All right. Is that a good way to manage and mitigate chemical facility terrorism risk?

Mr. WULF. Well, I think it is in that the facility, without the hardened security would, as a result of being tiered, have to look to implement security measures, develop a Site Security Plan that would bring it up to an acceptable level of security.

Mr. BEERS. The whole notion here is we want to level the playing field so——

Mr. HARPER. Sure, but——

Mr. BEERS [continuing]. A secure facility is great. An unsecured facility is something that we would want to change. We want to take the unsecured facility and raise it to roughly equivalent standards to the secure facility.

Mr. HARPER. But it appears to me that perhaps we are discouraging high-risk chemical facilities from increasing security at their facilities and making them stronger. And I don't know that that is having the desired effect that you are saying you want. Is it having that impact? And my time is up, so I guess I won't get a formal answer from you.

And I yield back.

Mr. SHIMKUS. The gentleman yields back his time.

And I see no other members. But before I dismiss the panel, I just want to reference the law. Because, Mr. Beers, you keep saying a consequence, which is something that we need to be concerned about. But that is not what the law says. The law says a risk-based system.

Mr. BEERS. Yes, sir.

Mr. SHIMKUS. Consequence is a part of that but it is not the whole calculation. I think you have caused more questions by this testimony today than answered questions.

So I think we will have them back, Mr. Ranking Member, to keep ferreting this out because the law is pretty clear. And you can see there are still a lot of questions on how we are trying to define this.

So we do thank you for coming. We do have the ability to offer written questions as the ranking member of the full committee asked. And with that, we would dismiss the first panel.

Mr. BEERS. Sir, may I respond to the question that you posed in writing?

Mr. SHIMKUS. Correct. You may. I would be happy to——

Mr. BEERS. I think if you are still not satisfied, then we have more work to do to——

Mr. SHIMKUS. I think you have a lot more work to do.

So we will dismiss this panel and we will have the second panel.

Staff, if I can get the back doors closed. Someone? Then we can move promptly.

We would like to continue the hearing and welcome our second panel, a one-member panel, so we can put full attention to the testimony and answer questions. So we would like to welcome Mr. Stephen Caldwell, Director of Homeland Security and Justice from the Government Accountability Office.

Sir, your full statement is in the record. You are recognized for 5 minutes.

STATEMENT OF STEPHEN L. CALDWELL, DIRECTOR, HOMELAND SECURITY AND JUSTICE, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. CALDWELL. Thank you very much, Chairman Shimkus and Ranking Member Tonko. I appreciate being here to talk about CFATS and the findings in our about-to-be released report on the program.

As you know, our earlier report focused on an internal DHS memo documenting management problems with the CFATS program and agency efforts to come up with corrective actions. But our current report focuses on agency efforts to do three things related to its core mission. The first of those is assess risks at the facility, which we have talked about quite a bit; review the Site Security Plans; and work with industry to improve security.

Let me start with the risk assessments. As noted, both the Department and GAO have established criteria for risk assessments and these were not followed closely in the CFATS program. Specifically, the three elements of risk—threat, vulnerability, and consequence—were not all used. As has been discussed, vulnerability has not been used even though DHS does collect extensive information on it. Some of the CFATS program criteria in its own 2007 rule, including the economic consequences, also have yet to be implemented.

Regarding the Site Security Plans, we found that the Department had a cumbersome process in place for reviewing the security plans which led to a backlog of security plans awaiting approval. The Department has attempted to streamline the review process by doing concurrent reviews among its experts when it had formerly been doing sequential reviews. However, the impacts of the streamlining is not known because no metrics were kept on how long the old process was taking.

But even with a more streamlined review process, as we have noted in our statement, we are estimating 7 to 9 years to improve those facilities that have been tiered. But our estimate does exclude some of the important parts of the regime as a whole, such as the compliance inspections.

Regarding industry, the CFATS program has increased its outreach, and this was noted in the inquiries we made through industry associations representing chemical facilities. The industry also expressed concerns about the burden of submitting and updating information to DHS, as well as frustration in wanting more details on the how and why the facilities were tiered a certain way. Some of these issues, as has been noted, may be resolved in terms of the Department is considering what information on its tiering process

it might provide to industry. Nevertheless, the CFATS program could benefit from systematically monitoring the effectiveness of its outreach activities.

In closing, I would like to briefly look back at our previous report, which commented on the serious management problems within the CFATS program. Because of a lack of documentation in the earlier years, we were really unable to determine the root causes for a lot of those problems. And this condition was found in our current work. As an example, we found no documentation as to why the current incomplete approach to risk assessment was chosen. So to some extent, the current program is still recovering from some of those earlier management problems.

But we have found the Department to be responsive to our recent recommendations and our current findings. We hope their positive attitude continues to result in improvements.

And related to this, I would like to note that my written statement is titled "Preliminary Observations." Because we are still awaiting Department comments on the recommendations in our current draft report, we will finalize that report once we receive those comments and we anticipate issuing that in early April.

With that, I am happy to respond to any questions.

[The prepared statement of Mr. Caldwell follows:]

United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Environment and the Economy, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, March 14, 2013

CRITICAL INFRASTRUCTURE PROTECTION

Preliminary Observations on DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach

Statement of Stephen L. Caldwell, Director
Homeland Security and Justice

GAO
Accountability * Integrity * Reliability

GAO-13-412T

GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-13-412T, a testimony before the Subcommittee on Environment and the Economy, Committee on Energy and Commerce, House of Representatives

Why GAO Did This Study

Facilities that produce, store, or use hazardous chemicals could be of interest to terrorists intent on using toxic chemicals to inflict mass casualties in the United States. As required by statute, DHS issued regulations that establish standards for the security of high-risk chemical facilities. DHS established the CFATS program in 2007 to assess the risk posed by these facilities and inspect them to ensure compliance with DHS standards. ISCD, which manages the program, places high-risk facilities in risk-based tiers and is to conduct inspections after it approves facility security plans. A November 2011 ISCD internal memorandum raised concerns about ISCD's ability to fulfill its mission.

This statement is based on GAO's ongoing work conducted for several congressional committees and subcommittees and provides preliminary observations regarding the extent to which DHS has (1) assigned chemical facilities to tiers and assessed its approach for doing so, (2) revised its process to review facility security plans, and (3) communicated and worked with owners and operators to improve security. To conduct this ongoing work, GAO reviewed DHS reports and plans on risk assessments, security plan reviews, and facility outreach and interviewed DHS officials. GAO received input from 11 trade associations representing chemical facilities about ISCD outreach. The results of this input are not generalizable but provide insights about DHS outreach efforts.

View GAO-13-412T. For more information, contact Stephen L. Caldwell, (202)-512-9610, CaldwellS@gao.gov

March 2013

CRITICAL INFRASTRUCTURE PROTECTION

Preliminary Observations on DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach

What GAO Found

Since 2007, the Department of Homeland Security's (DHS) Infrastructure Security Compliance Division (ISCD) has assigned about 3,500 high-risk chemical facilities to risk-based tiers under its Chemical Facilities Anti-Terrorism Standards (CFATS) program, but it has not fully assessed its approach for doing so. The approach ISCD used to assess risk and make decisions to place facilities in final tiers does not consider all of the elements of consequence, threat, and vulnerability associated with a terrorist attack involving certain chemicals. For example, the risk assessment approach is based primarily on consequences arising from human casualties, but does not consider economic consequences, as called for by the *National Infrastructure Protection Plan* (NIPP) and the CFATS regulation, nor does it include vulnerability, consistent with the NIPP. ISCD has begun to take some actions to examine how its risk assessment approach can be enhanced. Specifically, ISCD has, among other things, engaged Sandia National Laboratories to examine how economic consequences can be incorporated into ISCD's risk assessment approach and commissioned a panel of experts to assess the current approach, identify strengths and weaknesses, and recommend improvements. Given the critical nature of ISCD's risk assessment approach in laying the foundation for further regulatory steps in improving facility security, it is important that its approach for assigning facilities to tiers is complete within the NIPP risk management framework and the CFATS regulation.

DHS's ISCD has revised its process for reviewing facilities' site security plans—which are to be approved by ISCD before it performs compliance inspections—but it did not track data on the prior process so is unable to measure any improvements. The past process was considered by ISCD to be difficult to implement and caused bottlenecks in approving plans. ISCD views its revised process to be a significant improvement because, among other things, teams of experts review parts of the plans simultaneously rather than sequentially, as occurred in the past. Moving forward, ISCD intends to measure the time it takes to complete reviews, but will not be able to do so until the process matures. Using ISCD's expected plan approval rate of 30 to 40 plans a month, GAO estimated that it could take another 7 to 9 years before ISCD is able to complete reviews on the approximately 3,120 plans in its queue. ISCD officials said that they are exploring ways to expedite the process, such as reprioritizing resources.

DHS's ISCD has also taken various actions to work with facility owners and operators, including increasing the number of visits to facilities to discuss enhancing security plans, but trade associations that responded to GAO's query had mixed views on the effectiveness of ISCD's outreach. ISCD solicits informal feedback from facility owners and operators on its efforts to communicate and work with them, but it does not have an approach for obtaining systematic feedback on its outreach activities. Prior GAO work on customer service efforts in the government indicates that systematic feedback from those receiving services can provide helpful information as to the kind and quality of services they want and their level of satisfaction with existing services. GAO will continue to assess ISCD's efforts in these areas and consider any recommendations needed to address these issues. GAO expects to issue a report on its results in April 2013.

Chairman Shimkus, Ranking Member Tonko, and Members of the Subcommittee:

I am pleased to be here today to discuss our preliminary observations on the Department of Homeland Security's (DHS) efforts to address the various challenges in implementing and managing the Chemical Facility Anti-Terrorism Standards (CFATS) program. The events of September 11, 2001, triggered a national reexamination of the security of facilities that use or store hazardous chemicals in quantities that, in the event of a terrorist attack, could put large numbers of Americans at risk of serious injury or death. Chemicals held at these facilities can be used to cause harm to surrounding populations during terrorist attacks, can be stolen and used as chemical weapons or as precursors (the ingredients for making chemical weapons), or stolen and used to build an improvised explosive device. To mitigate this risk, the DHS appropriations act for fiscal year 2007[1] required DHS to issue regulations to establish risk-based performance standards for securing high-risk chemical facilities, among other things.[2] In 2007, DHS established the CFATS program to assess the risk, if any, posed by chemical facilities; place high-risk facilities in one of four risk-based tiers; require high-risk facilities to develop security plans; review these plans; and inspect the facilities to ensure compliance with the regulatory requirements. DHS's National Protection and Programs Directorate (NPPD) is responsible for the CFATS program. Within NPPD, the Infrastructure Security Compliance Division (ISCD), a division of the Office of Infrastructure Protection (IP), manages the program.

In 2011, a leaked internal memorandum prompted some Members of Congress and chemical facility owners and operators to become concerned about ISCD's ability to implement and manage a regulatory regime under the CFATS program. In July 2012, we reported that ISCD had efforts under way to address the problems highlighted in the internal memorandum and had developed an action plan to track its progress on

[1]Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388 (2006).

[2]According to DHS, a high-risk chemical facility is one that, in the discretion of the Secretary of Homeland Security, presents a high risk of significant adverse consequences for human life or health, national security, or critical economic assets if subjected to a terrorist attack, compromise, infiltration, or exploitation. 6 C.F.R. § 27.105.

various human capital, mission, and administrative issues.[3] As requested, this testimony discusses our preliminary observations on the extent to which DHS has (1) assigned chemical facilities to risk-based tiers and assessed its approach for doing so, (2) revised the process used to review security plans, and (3) communicated and worked with facilities to help improve security.

My statement today is based on preliminary analyses from our ongoing review of the CFATS program for a number of congressional committees and subcommittees.[4] We expect to issue a final report on this work in April 2013. To conduct this work, we are reviewing the CFATS statute and regulation;[5] the *National Infrastructure Protection Plan* (NIPP);[6] as well as applicable ISCD policies, processes, and procedures. We are reviewing and analyzing ISCD documents including the web-based tools used to collect security information from facilities, the ISCD risk assessment approach used to determine a facility's risk, and data ISCD collects from facilities to assign them to risk-based tiers. We are also reviewing documents such as the November 2011 internal memorandum and ISCD security plan review policies and procedures. To confirm our understanding of the security plan review process, we are also gathering and analyzing statistics to determine how many security plans have been reviewed, authorized, and approved from program inception through

[3]GAO, *Critical Infrastructure Protection: DHS Is Taking Action to Better Manage Its Chemical Security Program, but It Is Too Early to Assess Results*, GAO-12-515T (Washington, D.C.: July 26, 2012). This report was summarized in *Critical Infrastructure Protection: Summary of DHS Actions to Better Manage Its Chemical Security Program*, GAO-12-1044T (Washington D.C. Sept. 20, 2012).

[4]These committees and subcommittees include the Senate Committees on Homeland Security and Governmental Affairs; Commerce, Science, and Transportation; the Judiciary; and Environment and Public Works, Subcommittee on Superfund, Toxics, and Environmental Health; as well as the House Committees on Appropriations, Subcommittee on Homeland Security; Homeland Security; Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies; Energy and Commerce; and Energy and Commerce, Subcommittee on Environment and the Economy. Two individual Members of Congress are also requesters for this work.

[5]Throughout this statement, we used the terms "regulation" or "rule" interchangeably when referring to the CFATS regulation.

[6]DHS, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006). DHS updated the NIPP in January 2009 to include resiliency. See DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009). The NIPP sets forth the risk management framework for the protection and resilience of the nation's critical infrastructure.

December 2012. Regarding communicating and working with facilities to improve security, we contacted officials representing 15 trade associations with members regulated by CFATS to obtain their perspectives on DHS efforts to work with facility owners and operators.[7] Out of these 15 associations, 11 responded, and the information we obtained from them is not generalizable to the universe of chemical facilities covered by CFATS; however, it provides insights into DHS efforts to perform outreach and seek feedback on the implementation of the CFATS rule. We assessed the reliability of the data we used for this statement and found that the data were sufficiently reliable for the purposes of this statement. We also interviewed ISCD officials responsible for overseeing the CFATS program to confirm our understanding of the documents and data provided. We shared the information in this statement with DHS officials and incorporated its comments where appropriate. We are conducting our work in accordance with generally accepted government auditing standards.

Background

Section 550 of the DHS appropriations act for fiscal year 2007[8] requires DHS to issue regulations establishing risk-based performance standards for the security of facilities that the Secretary determines to present high levels of security risk, among other things.[9] The CFATS rule was published in April 2007,[10] and appendix A to the rule, published in November 2007, listed 322 chemicals of interest and the screening

[7]We selected these 15 trade associations because they are listed in the NIPP as those with which DHS works on a regular basis on chemical security matters. According to the NIPP, working with these trade associations presents a more manageable number of contact points through which DHS can coordinate activities with a large number of the asset owners and operators in the chemical sector.

[8]Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388 (2006).

[9]The CFATS rule establishes 18 risk-based performance standards that identify the areas for which a facility's security posture are to be examined, such as perimeter security, access control, and cyber security. To meet these standards, facilities are free to choose whatever security programs or processes they deem appropriate so long as DHS determines that the facilities achieve the requisite level of performance in each applicable standard.

[10]72 Fed. Reg. 17,688 (Apr. 9, 2007) (codified at 6 C.F.R. pt. 27).

threshold quantities for each.[11] ISCD has direct responsibility for implementing DHS's CFATS rule, including assessing potential risks and identifying high-risk chemical facilities, promoting effective security planning, and ensuring that final high-risk facilities meet applicable standards through site security plans approved by DHS. From fiscal years 2007 through 2012, DHS dedicated about $442 million to the CFATS program. During fiscal year 2012, ISCD was authorized 242 full-time-equivalent positions.

ISCD uses a risk assessment approach to develop risk scores to assign chemical facilities to one of four final tiers. Facilities placed in one of these tiers (tier 1, 2, 3, or 4) are considered to be high risk, with tier 1 facilities considered to be the highest risk. According to an ISCD document that describes how ISCD develops its CFATS risk score, the risk score is intended to be derived from estimates of consequence (the adverse effects of a successful attack), threat (the likelihood of an attack), and vulnerability (the likelihood of a successful attack, given an attempt). ISCD's risk assessment approach is composed of three models, each based on a particular security issue: (1) release, (2) theft or diversion, and (3) sabotage, depending on the type of risk associated with the 322 chemicals.[12] Once ISCD estimates a risk score based on these models, it assigns the facility to a final tier.

[11]72 Fed. Reg. 65,396 (Nov. 20, 2007). According to DHS, CFATS not only covers facilities that manufacture chemicals but also covers facilities that store or use certain chemicals as part of their daily operations. This can include food-manufacturing facilities that use chemicals of interest in the manufacturing process, universities that use chemicals to do experiments, or warehouses that store ammonium nitrate, among others.

[12]For release, the model assumes that a terrorist will release the chemical of interest at the facility and then estimates the risk to the surrounding population. For theft or diversion, the model assumes that a terrorist will steal or have the chemical of interest diverted to him or herself and then estimates the risk of a terrorist attack using the chemical of interest in a way that causes the most harm at an unspecified off-site location. For sabotage, the model assumes that a terrorist will remove the chemical of interest from the facility and mix it with water, creating a toxic release at an unspecified off-site location, and then estimates the risk to a medium-sized U.S. city.

ISCD Has Assigned Thousands of Facilities to Tiers, but ISCD's Approach to Risk Assessment Does Not Reflect All Risk Elements

ISCD Has Tiered Thousands of High-Risk Chemical Facilities and Resolved Some Problems Using Its Risk Assessment Approach to Assign Tiers

In July 2007, ISCD began reviewing information submitted by the owners and operators of approximately 40,000 facilities. By January 2013, ISCD had designated about 4,400 of the 40,000 facilities as high risk and thereby covered by the CFATS rule.[13] ISCD had assigned about 3,500 of those facilities to a final tier, of which about 90 percent were tiered because of the risk of theft or diversion. The remaining 10 percent were tiered because of the risk of release or the risk of sabotage.[14]

Over the last 2 years, ISCD has identified problems with the way the release chemicals model assigns chemical facilities to tiers and has taken or begun to take action to address those problems. In February 2011, ISCD found that some chemical facilities had been placed in an incorrect final tier because this model included incorrect data about the release of high-risk chemicals of interest. In June 2011, ISCD officials adjusted the model, which resulted in lowering the tier for about 250 facilities, about 100 of which were subsequently removed from the CFATS program. In October 2012, ISCD officials stated that they had uncovered another defect that led the model to exclude population density calculations for about 150 facilities in states or U.S. territories outside the continental United States, including Alaska, Hawaii, Puerto Rico, and Guam. In

[13]According to ISCD officials, approximately 35,600 facilities were not considered high risk because after preliminary evaluation, DHS concluded that they were considered not to be high enough risk to be covered by the program; thus they were no longer covered by the rule.

[14]According to ISCD officials, depending on the chemicals on-site, a facility can be final-tiered for more than one security issue.

February 2013, ISCD officials said that they had made adjustments to the model to resolve this issue and do not expect any facilities' tier will change due to this issue.

ISCD's Risk Assessment Approach Does Not Consider All Elements of Risk

Our preliminary analyses indicates that the tiering approach ISCD uses to assess risk and assign facilities to final tiers does not consider all of the elements of risk associated with a terrorist attack involving certain chemicals. According to the NIPP, which, among other things, establishes the framework for managing risk among the nation's critical infrastructure, risk is a function of three components—consequence, threat, and vulnerability—and a risk assessment approach must assess each component for every defined risk scenario. Furthermore, the CFATS rule calls for ISCD to review consequence, threat, and vulnerability information in determining a facility's final tier. However, ISCD's risk assessment approach does not fully consider all of the core criteria or components of a risk assessment, as specified by the NIPP, nor does it comport with parts of the CFATS rule.

- *Consequence*. The NIPP states that at a minimum, consequences should focus on the two most fundamental components—human consequences and the most relevant direct economic consequences. The CFATS rule states that chemical facilities covered by the rule are those that present a high risk of significant adverse consequences for human life or health, or critical economic assets, among other things, if subjected to terrorist attack, compromise, infiltration, or exploitation.[15] Our review of ISCD's risk assessment approach and discussions with ISCD officials shows that the approach is currently limited to focusing on one component of consequences—human casualties associated with a terrorist attack involving a chemical of interest—and does not consider consequences associated with economic criticality. ISCD officials said that the economic consequences part of their risk-tiering approach will require additional work before it is ready to be introduced. In September 2012, ISCD officials stated that they had engaged Sandia National Laboratories to examine how ISCD could gather needed information and determine the risk associated with economic impact, but this effort is in the initial

[15] 6 C.F.R. §§ 27.105, .205.

stages, with an expected completion date of June 2014.[16] ISCD officials added they are uncertain about how Sandia's efforts will affect their risk assessment approach.

- *Threat.* ISCD's risk assessment approach is also not consistent with the NIPP because it does not consider threat for the majority of regulated facilities. According to the NIPP, risk assessments should estimate threat as the likelihood that the adversary would attempt a given attack method against the target. The CFATS rule requires that, as part of assessing site vulnerability, facilities conduct a threat assessment, which is to include a description of the internal, external, and internally assisted threats facing the facility and that ISCD review site vulnerability as part of the final determination of a facility's tier.[17] Our review of the models and discussions with ISCD officials shows that (1) ISCD is inconsistent in how it assesses threat using the different models because while it considers threat for the 10 percent of facilities tiered because of the risk of release or sabotage, it does not consider threat for the approximately 90 percent of facilities that are tiered because of the risk of theft or diversion; and (2) ISCD does not use current threat data for the 10 percent of facilities tiered because of the risk of release or sabotage. ISCD did not have documentation to show why threat had not been factored into the formula for approximately 90 percent of facilities tiered because of the risk of theft or diversion. However, ISCD officials pointed out that the cost of adding a threat analysis for these facilities might outweigh the benefits of doing so. ISCD officials said that given the complexity of assessing threat for theft or diversion, they are considering reexamining their approach. ISCD officials also said that they are exploring how they can use more current threat data for the 10 percent of facilities tiered because of the risk of release or sabotage.

- *Vulnerability.* ISCD's risk assessment approach is also not consistent with the NIPP because it does not consider vulnerability when developing risk scores. According to the NIPP, risk assessments should identify vulnerabilities, describe all protective measures, and

[16]Sandia National Laboratories is a Federally Funded Research and Development Center of the Department of Energy that provides independent consulting services to DHS with regard to modeling, simulation, and analysis of risk-based assessments among other things.

[17]6 C.F.R. §§ 27.215, .220.

estimate the likelihood of an adversary's success for each attack scenario. Similar to the NIPP, the CFATS rule calls for ISCD to review facilities' security vulnerability assessments as part of its risk-based tiering process.[18] This assessment is to include the identification of potential security vulnerabilities and the identification of existing countermeasures and their level of effectiveness in both reducing identified vulnerabilities and meeting the aforementioned risk-based performance standards. Our review of the risk assessment approach and discussions with ISCD officials shows that the security vulnerability assessment contains numerous questions aimed at assessing vulnerability and security measures in place but the information is not used to assign facilities to risk-based tiers. ISCD officials said they do not use the information because it is "self-reported" by facilities and they have observed that it tends to overstate or understate vulnerability. As a result, ISCD's risk assessment approach treats every facility as equally vulnerable to a terrorist attack regardless of location and on-site security. ISCD officials told us that they consider facility vulnerability, but at the latter stages of the CFATS regulatory process particularly with regard to the development and approval of the facility site security plan.

ISCD Has Begun to Take Actions to Examine How Its Approach Could Be Enhanced

Our preliminary work indicates that ISCD has begun to take some actions to examine how its risk assessment approach can be enhanced. For example, in addition to engaging Sandia National Laboratories to develop the framework for assessing economic consequences previously discussed, ISCD has commissioned a panel of subject matter experts to examine the strengths and weaknesses of its current risk assessment approach. ISCD officials stated that the panel's work is intended to focus on whether ISCD is heading in the right direction, and they view it as a preliminary assessment. According to ISCD's task execution plan, the panel is to provide actionable recommendations on potential improvements to the CFATS models, but the panel is not to develop alternative CFATS models or formally validate or verify the current CFATS risk assessment approach—steps that would analyze the structure of the models and determine whether they calculate values correctly. In February 2013, after the panel was convened, ISCD officials stated that they provided information to the panel about various issues that they might want to consider, among them, (1) how to address

[18] 6 C.F.R. § 27.220.

vulnerability in the models given ISCD concerns about data quality, and (2) what the appropriate variables to use, if any, are for threats associated with theft or diversion, as discussed earlier.

We believe that ISCD is moving in the right direction by commissioning the panel to identify the strengths and weaknesses of its risk assessment approach, and the results of the panel's work could help ISCD identify issues for further review and recommendations for improvement. Given the critical nature of ISCD's risk assessment approach in laying the foundation for further regulatory steps in improving facility security—such as the development and approval of facility site security plans—it is important that its approach for assigning facilities to tiers is complete within the NIPP risk management framework and the CFATS rule. Once ISCD's develops a more complete approach for assessing risk it would then be better positioned to commission an independent peer review. In our past work, we reported that peer reviews are a best practice in risk management[19] and that independent expert review panels can provide objective reviews of complex issues.[20] Furthermore, the National Research Council of the National Academies has recommended that DHS improve its risk analyses for infrastructure protection by validating the models and submitting them to external peer review.[21] As we have previously reported, independent peer reviews cannot ensure the success of a risk assessment approach, but they can increase the probability of success by improving the technical quality of projects and the credibility of the decision-making process.[22] We will continue to monitor and assess ISCD's efforts to examine its risk assessment approach through our

[19]See GAO, *Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*, GAO-12-14 (Washington, D.C.: Nov. 17, 2011). Peer reviews can identify areas for improvement and can facilitate sharing best practices.

[20]See GAO, *Aviation Security: Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges*, GAO-10-763 (Washington, D.C.: May 20, 2011).

[21]National Research Council of the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis*. (Washington, D.C. 2010).

[22]See GAO-12-14 and GAO, *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T (Washington D.C.: Mar. 31, 2004).

ongoing work and consider any recommendations needed to address these issues.

ISCD Revised Its Security Plan Review Process, but Plan Approvals Could Take Years

ISCD Revised Its Security Plan Review Process because of ISCD Managers' Concerns, and Plans to Measure Related Improvements Moving Forward

Our preliminary work shows that ISCD has made various revisions to its security plan review process to address concerns expressed by ISCD managers about slow review times. Under the CFATS rule, once a facility is assigned a final tier, it is to submit a site security plan to describe security measures to be taken and how it plans to address applicable risk-based performance standards.[23] The November 2011 internal memorandum that discussed various challenges facing the CFATS program noted that ISCD had not approved any security plans and stated that the process was overly complicated and created bottlenecks. The memorandum stated that revising the process was a top program priority because the initial security plan reviews were conducted using the risk-based standards as prescriptive criteria rather than as standards for developing an overall facility security strategy.[24]

According the ISCD officials, the first revision was called the interim review process, whereby individual reviewers were to consider how layers of security measures met the intent of each of the 18 standards. Under the interim review process, ISCD assigned portions of each facility's plan

[23]6 C.F.R. § 27.210(a)(3), .225.

[24]The specific security measures and practices discussed in DHS's guidelines state that they are neither mandatory nor necessarily the "preferred solution" for complying with the risk-based performance standards. Rather, according to DHS, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the standards. High-risk facility owners and operators have the ability to choose and implement other measures to meet the risk-based performance standards based on circumstances, security issues and risks, and other factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the standards.

to security specialists (e.g., cyber, chemical, and physical, among others) who reviewed plans in a sequential, linear fashion. Using this approach, plans were reviewed by different specialists at different times culminating in a quality review. ISCD officials told us that the interim review process was unsustainable, labor-intensive, and time-consuming, particularly when individual reviewers were looking at pieces of thousands of plans that funneled to one quality reviewer.[25] In July 2012, ISCD stopped using the interim review process and began using the current revised process, which entails using contractors, teams of ISCD employees (physical, cyber, chemical, and policy specialists), and ISCD field office inspectors, who are to review plans simultaneously.

ISCD officials said that they believe the revised process for reviewing security plans is a "quantum leap" forward, but they did not capture data that would enable them to measure how, if at all, the revised process is more efficient (i.e., less time-consuming) than the former processes. They said that, under the revised process, among other things, field inspectors are to work with facilities with the intent of resolving any deficiencies ISCD identifies in their site security plans. They added that this contrasts with past practices whereby ISCD would review the entire plan even when problems were identified early and not return the plan to the facility until the review was complete, resulting in longer reviews. Moving forward, ISCD officials said they intend to measure the time it takes to complete parts of the revised process and have recently implemented a plan to measure various aspects of the process. Specifically, ISCD's *Annual Operating Plan*, published in December 2012, lists 63 performance measures designed to look at various aspects of the site security plan review process—from the point the plans are received by ISCD to the point where plans are reviewed and approved. Collecting data to measure performance about various aspects of the security plan review process is a step in the right direction, but it may take time before the process has matured to the point where ISCD is able to establish baselines and assess its progress.

[25]Using the interim review process, ISCD officials estimated that they authorized about 60 security plans and notified the facilities that inspectors would schedule visits to determine if the security measures described in the plan were in place.

Security Plan Reviews Could Take Years to Complete, but ISCD Is Examining How It Can Accelerate the Review Process

ISCD has taken action to improve its security plan review process, but based on our preliminary analysis, it could take years to review the plans of thousands of facilities that have already been assigned a final tier. ISCD hopes to address this by examining how it can further accelerate the review process. According to ISCD officials, between July 2012 and December 2012, ISCD had approved 18 security plans, with conditions.[26] ISCD officials told us that, moving forward, they anticipate that the revised security plan review process could enable ISCD to approve security plans at a rate of about 30 to 40 a month.

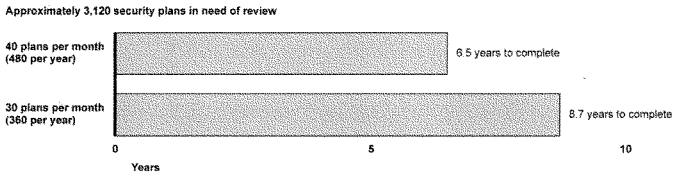
Using ISCD's estimated approval rate of 30 to 40 plans a month, our preliminary analysis indicates that it could take anywhere from 7 to 9 years to complete reviews and approvals for the approximately 3,120 plans[27] submitted by facilities that have been final-tiered that ISCD has not yet begun to review.[28] Figure 1 shows our estimate of the number of years it could take to approve all of the security plans for the approximately 3,120 facilities that, as of January 2013, had been final-tiered, assuming an approval rate of 30 to 40 plans a month.

[26]All authorization letters include a condition noting that ISCD has not fully approved the personnel surety risk-based performance standard of plans because ISCD has not yet determined what the facilities are to do to meet all aspects of personnel surety. The personal surety risk-based performance standard requires that regulated chemical facilities implement measures designed to identify people with terrorist ties, among other things.

[27]ISCD data show that 380 security plans have started the review process and are at different phases of review.

[28]ISCD officials stated that the approval rate could reach 50 plans a month in the third quarter of fiscal year 2013, as the review process becomes more efficient. We did not calculate the time to complete reviews of the approximately 3,120 plans that had been final-tiered using ISCD's estimate of 50 per month because of uncertainty over when and if ISCD would reach this goal during the third quarter of fiscal year 2013.

Figure 1: Preliminary Estimate of Number of Years to Approve Security Plans



Source: GAO.

It is important to note that our 7- to 9-year preliminary estimate does not include other activities central to the CFATS mission, either related to or aside from the security plan review process. In addition, our estimate does not include developing and implementing the compliance inspection process, which occurs after security plans are approved and is intended to ensure that facilities that are covered by the CFATS rule are compliant with the rule, within the context of the 18 performance standards. According to ISCD officials, they are actively exploring ways to expedite the speed with which the backlog of security plans could be cleared, such as potentially leveraging alternative security programs, reprioritizing resources, and streamlining the inspection and review requirements. ISCD officials added that they plan to complete authorizations inspections and approve security plans for tier 1 facilities by the first quarter of fiscal year 2014 and for tier 2 facilities by the third quarter of fiscal year 2014.

ISCD Has Increased Its Efforts to Communicate and Work with Facilities, but Does Not Solicit Systematic Feedback on Effectiveness of Its Outreach

ISCD's External Communication Efforts with Facilities Have Increased since 2007, but Selected Trade Associations Had Mixed Views about ISCD Efforts

Our preliminary work shows that ISCD's efforts to communicate and work with owners and operators to help them enhance security at their facilities have increased since the CFATS program's inception in 2007, particularly in recent years. Since 2007, ISCD has taken various actions to communicate with facility owners and operators and various stakeholders—including officials representing state and local governments, private industry, and trade associations—to increase awareness about CFATS. From fiscal years 2007 through 2009, most of ISCD's communication efforts entailed outreach with owners and operators and stakeholders through presentations to familiarize them with CFATS; field visits with federal, state, and local government and private industry officials; and compliance assistance visits at facilities that are intended to assist facilities with compliance or technical issues. By 2010 and in subsequent years, ISCD had revised its outreach efforts to focus on authorization inspections during which inspectors visited facilities to verify that the information in their security plans was accurate and complete, and other outreach activities including stakeholder outreach.[29]

[29]Among other outreach activities, ISCD manages the Chemical Security website, which includes a searchable database to answer questions about the CFATS program. ISCD also manages a Help Desk (call service center), which it operates on a contract basis by the Oak Ridge National Laboratory. According to ISCD, from April 2007 through July 2012, the Help Desk responded to nearly 80,000 user inquires, submitted via telephone, e-mail and fax. We did not review the quality of the responses provided through the help desk function or assess the qualifications of the staff responding to user inquires because doing so was outside of the scope of this review.

However, analysis of industry trade associations' responses to questions we sent them about the program shows mixed views about ISCD's efforts to communicate with owners and operators through ISCD outreach efforts. For example, 3 of the 11 trade associations that responded to our questions indicated that ISCD's outreach program was effective in general, 3 reported that the effectiveness of ISCD's outreach was mixed, 4 reported that ISCD's outreach was not effective, and 1 respondent reported that he did not know.[30]

ISCD Seeks Informal Feedback, but Does Not Solicit Systematic Feedback on the Effectiveness of Its Outreach Efforts

Our preliminary results indicate that ISCD seeks informal feedback on its outreach efforts but does not systematically solicit feedback to assess the effectiveness of outreach activities,[31] and it does not have a mechanism to measure the effectiveness of ISCD's outreach activities. Trade association officials reported that in general ISCD seeks informal feedback on its outreach efforts and that members provide feedback to ISCD. Association officials further reported that among other things ISCD has encouraged association members to contact local ISCD inspectors and has hosted roundtable discussions and meetings where members of the regulated community provide feedback, suggest improvements, or make proposals regarding aspects of the CFATS program such as site security plans, alternative security programs, and gasoline storage site risks. Furthermore, according to ISCD officials, while feedback is solicited from the regulated community generally on an informal basis, inspectors and other staff involved in ISCD's outreach activities are not required to solicit feedback during meetings, presentations, and assistance visits, and inspectors are also not required to follow up with the facilities after compliance assistance visits to obtain their views on the effectiveness of the outreach.

[30]We originally sent questions to 15 trade associations representing various members of the chemical industry and received responses from 11 of the 15. The trade associations that responded provided responses that represent, to their knowledge, the general view of their members. In some instances the associations provided responses directly from member companies.

[31]ISCD solicits voluntary feedback via a three-question survey provided to Help Desk users on their experience with call center representatives. The survey asks three questions: Did the service meet expectations, were questions answered in a timely manner, and was the call service representative friendly and knowledgeable.

ISCD, as part of its annual operating plan, has established a priority for fiscal year 2013 to develop a strategic communications plan intended to address external communication needs including industry outreach. We have previously reported on the benefits of soliciting systematic feedback. Specifically, our prior work on customer service efforts in the government indicates that systematic feedback from those receiving services can provide helpful information as to the kind and quality of services they want and their level of satisfaction with existing services. We will continue to monitor and assess ISCD's efforts to develop a systematic way to solicit feedback through our ongoing work and consider any recommendations needed to address this issue.

Chairman Shimkus, Ranking Member Tonko, and members of the subcommittee, this completes my prepared statement. I would be happy to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgments

For information about this statement please contact Stephen L. Caldwell, at (202) 512-9610 or CaldwellS@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Other individuals making key contributions included John F. Mortin, Assistant Director; Chuck Bausell; Jose Cardenas; Michele Fejfar; Jeff Jensen; Tracey King; Marvin McGill; Jessica Orr; and Ellen Wolfe.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission	The Government Accountability 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 GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Website: http://www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Please Print on Recycled Paper.

Mr. SHIMKUS. Thank you, Mr. Caldwell.

I would like to recognize myself for 5 minutes for the first round of questions.

You were in here for the last panel and probably listened to my last exchange based upon the language of the law. Could you understand my frustration with the question based upon what members had said before about the formula for risk and if there are two variables that are undefined, how do you identify risk?

Mr. CALDWELL. Yes. I guess I agree with your point. The law calls for an assessment of risk, not of consequence. I think the DHS response we have heard today kind of indicates that the exclusion of vulnerability was part of a well-laid-out and thoughtful methodology and analysis that they used from the start. We certainly found no evidence of this. I mean our early discussions with methodology with them last year indicated the fissures did not know why the current methodology was picked or why vulnerability was left out. And there certainly was no documentation on that. It was really only when we raised the issue of the lack of the consideration of vulnerability——

Mr. SHIMKUS. It was?

Mr. CALDWELL [continuing]. That the current narrative emerged that you heard today. So I think that really reinforces the need for an independent peer review, preferably earlier in the process than now because the problems they will have if they find major changes. And I have some other comments on peer review I can make as well.

Mr. SHIMKUS. Did you get any comfort from the response that the formula is being reviewed by Sandia? And I think the frustration from my end was that we might take it; we might consider it. I mean, it was pretty vague as to whether all of this work that they would even consider is part of a fix to the formula.

Mr. CALDWELL. Yes. Let me make two comments on the peer review. I think based on our work today—and they have been sharing a lot of information with us—but we are still not sure how much of a free hand and leeway this new peer review is going to have, this expert panel. Will they have the leeway to really start from scratch and kind of come up with fundamental changes from the model if they think they are needed?

And then, of course, we are also not really sure and the Department really hasn't committed to really how they would receive any major recommendations for changes because of impacts it could have on the peering process. So that is what I will call the peer review's need to do a review of the methodology.

But what the peer review would also need to do to be comprehensive would be what is called the V and V, or a verification and validation. We know that there was some miscalculations found in the formula. This did lead to the re-tiering of several facilities. Also, in the course of our work, we found out there was an omission of certain locations such as Hawaii, Alaska, and Puerto Rico from the data in the model calculations. And they don't think this will lead to any changes in tiering, but, I mean, together they certainly don't give us a warm, fuzzy feeling that they have looked at the actual mechanics of the model to make sure that even if the methodology is correct that the model is working the way it was intended to. So

it is also important that the peer review do a V and V, a verification and validation, to actually look at the model, play with the numbers, do calculations, ensure they are correct, and maybe do some sensitivity analysis as well.

Mr. SHIMKUS. Well, and just kind of following up on this line of questions because it was asked by one of my colleagues on data, data collection, and what is it used for. Again, a pretty vague answer by our first panel as to what they really needed, what they had, and why they had it. You found that owners and operators were spending unnecessary resources complying with CFATS data collection requirements. Can you elaborate on your findings?

Mr. CALDWELL. Well, I will say two things. I think whether the industry feels that they misspent funds or wasted funds, I will leave maybe for the third panel. You can ask them that. But in terms of the question about whether all this vulnerability data was useful that the Department is capturing but is not using, I think the way they put it is that it is data that then the facilities have been able to use or could use. So again, that is a question for the facilities. I mean, you could ask the facilities and industry——

Mr. SHIMKUS. But the facilities are the ones who provide the data. So it is kind of like we got the data, we gave it to Homeland Security, and then Homeland Security says we got the data, here is your data because it is going to help you out, or the collection of that data will help you out. I mean, it is just——

Mr. CALDWELL. Yes.

Mr. SHIMKUS [continuing]. Counterintuitive. I am struggling with this.

Mr. CALDWELL. We found that the Department is not using the vulnerability data at all that it collected from facilities.

One other thing on that point, when we talked to them about why they were not using the vulnerability data, they said, well, they were concerned because it was self-reported and thus might be either exaggerated or not exaggerated. But everything in this thing is self-reported until—I mean everything going into tiering about how much chemicals they have and where they have them and the method of storage—all of that is self-reported. So I am not sure that I agree with that distinction.

Mr. SHIMKUS. You are not helping me very much but thank you. My frustration level continues to mount.

So I would like to recognize the ranking member, Mr. Tonko, for 5 minutes.

Mr. TONKO. Thank you, Mr. Chairman. I hope you can relax for a moment.

I thank you, Mr. Caldwell, for appearing here today.

GAO's analysis reveals significant concerns about this important national security program and the sufficiency of the Department of Homeland Security's Action Plan to address these concerns. We heard from the Department on the first panel that they are taking GAO's findings seriously and intend to follow GAO's recommendations to strengthen the risk assessment models used in their programs.

It seems that some of these concerns are long-standing. For instance, stakeholders have long called for a greater transparency in the risk assessment process. I welcome the GAO's testimony today

and have a few questions that, I think, would be helpful in providing the information we require. To the DHS methodology itself, does it appropriately, in your opinion, account for threat?

Mr. CALDWELL. Threat is a little tougher. And so I think in our own analysis we have been less critical of the Department on that. And the reason that threat is more difficult is because the threat comes from a potentially adaptive adversary that can see where vulnerabilities have been reduced or maybe where vulnerabilities still exist and change their targets. But even more so, when you are looking at these chemical facilities, the facilities themselves could be attacked or some of the chemicals at those facilities could be stolen or diverted and then moved and then used again in a population center or any other location. So I think it is very difficult, and also I think in terms of some of the questions about threat there were asked, there just really is not a lot of actionable, real intelligence that shows there is a threat against these facilities or specific facilities.

Mr. TONKO. Thank you. And to that methodology again, does it account for the two minimum components of consequences, that being human consequences and economic consequences?

Mr. CALDWELL. It does not include economic consequences. As the Department has stated, they have now engaged Sandia National Labs to do that but it has been a while. I mean, the rule came out in 2007 that specifically said that they would include that at some point. And if you look at the National Infrastructure Protection Plan it does say at a minimum consequence needs to include both human casualties and fatalities, those things, as well as the economic consequences.

Mr. TONKO. Thank you. And I would imagine that GAO has looked at risk assessments prepared by many different agencies over the years. How would you say the CFATS risk assessments compare to the work at those other agencies?

Mr. CALDWELL. Well, there are a couple of examples I can think of. At the Coast Guard, for example, we have done extensive work on their risk assessment model. It is called the Maritime Security Risk Assessment Model. And it does include all the components. And that is probably the most sophisticated model within DHS because it also takes into account the mitigation efforts that a facility is doing and how that impacts the risk.

There have been other cases—I believe it is TSA—I will have to correct my statement if I find that it is a different agency—where we found that vulnerability was also being held constant and we have made those recommendations that they not do that and that that particular component agreed with that recommendation.

Mr. TONKO. Thank you. During the first panel Director Wulf indicated that including vulnerability in risk assessments would lead to an ever-changing tier assignment for a given facility. Is this a valid enough reason for leaving the criteria out of the assessment?

Mr. CALDWELL. Well, I think if in the beginning that was thought through and done on purpose, I could have maybe given him a little more sympathy if he is trying to design something to do that. But as I said, that narrative was developed pretty recently as to why was left out. There is a problem now in that a lot of these facilities, thousands of these facilities—and if there are major

changes in their model because of the peer review or things we have said or adding the economic consequences, this could reasonably change the tiering of those facilities.

Mr. TONKO. And this committee is aware of two mis-tiering incidences at the Department were facilities where placed in the wrong tier because of errors made by the Department. That is a serious problem. But now we hear from GAO that none of the more than 3,500 tiering decisions that have been made are reliable. They are all based on a risk assessment methodology that is seriously lacking. Is that an accurate assessment?

Mr. CALDWELL. I wouldn't use the term that this is a fatal flaw or things like that. But certainly we are questioning why they haven't included vulnerability. I think that we have a concern. Now, we do believe the best way to address that would be to have a peer review come in externally, review it. As we have said before, and as you said before, the National Academies of Sciences came in and found very similar problems across the Department that we are talking about here within the CFATS program.

Mr. TONKO. Well, I see that my time has expired so I will yield back, Mr. Chairman.

Mr. SHIMKUS. Thank you.

The chair now recognizes the gentleman from Pennsylvania, Mr. Pitts, for 5 minutes.

Mr. PITTS. Thank you, Mr. Chairman.

Mr. Caldwell, you noted in your statement that it could take 7 to 9 years before ISCD completes the review of the 3,120 security plans currently in the review queue and that the estimate does not include work by ISCD on other missioned activities. What are some examples of these ISCD activities?

Mr. CALDWELL. Well, that estimate does not include about 900 facilities that have yet to be assigned into a final tier. Also, the time required to review the plans to resolve issues related to personnel surety take some time because some of the plans have been provisionally or conditionally approved. So they have to go back and revisit that once the personnel surety rule is in place. And then there are the compliance inspections that they would do which are separate from the plan approval, but those are generally done a year after. So you are looking at another year out there for individual facilities before they have the compliance inspections. And really, it is only until you have the compliance inspection whether you know that the facility is actually implementing the things in its security plan.

Mr. PITTS. So will implementing these mission activities further delay full CFATS program implementation?

Mr. CALDWELL. Well, certainly until all of the pieces are in place, it is not going to be there. And I think several figures have been thrown out; 8 to 10 years we said in our last hearing. I mean, now, we are looking at 7 to 9 just for the approval plan. So it is going to be some time before this regime is completely in place. It is in contrast to maybe some of the other programs that were put in place after 9/11.

Mr. PITTS. Now, the regulated industry says that ISCD's efforts to communicate regarding CFATS-related issues are mixed in effec-

tiveness. Does ISCD measure the effectiveness of its outreach efforts and could they?

Mr. CALDWELL. No, they don't. They measure some of the things like how many meetings they have and those kinds of things, but they haven't outreached really to find out whether these have been effective so we are considering——

Mr. PITTS. Should they or could they?

Mr. CALDWELL. Yes. And we are considering a recommendation with the Department. We are in discussions with a recommendation that we ask that they do so.

Mr. PITTS. What should we take away from the input that you got from trade associations?

Mr. CALDWELL. Some of the things are working pretty well. The meetings with this Sector Coordinating Council seem to be effective according to industry. Also some of the visits to facilities, a little bit mixed there. I think the more recent things based on some of the testimony you will hear later today is that the officials doing those inspections from DHS do seem qualified and helpful, whereas I think some of the early responses that they were very reluctant to actually make useful concrete suggestions on how to improve security.

Mr. PITTS. Now, you found that owners and operators were spending unnecessary resources complying with CFATS data collection requirements. Would you elaborate on that?

Mr. CALDWELL. I don't believe we ever said they were unnecessary. I just think they were worried about a substantial burden in terms of the cost it was taking to do these, particularly, if something changed and they did this. I think one of the things industry may tell you about in the next panel is the chemical industry can be a complicated business, so sometimes they change mixes of their chemicals in terms of some of their processes. And there has been a debate about whether then do they have to go back to DHS and resubmit everything because their mixture of chemicals is slightly different? It is a concern.

Mr. PITTS. And what in your view is the difference between the current Site Security Plans and Alternative Security Plans?

Mr. CALDWELL. Well, I think the Alternative Security Plans look a little simpler. I think that they have some of the same information but perhaps in a more useful way because it is portrayed as a plan as opposed to a data dump of a lot of individual information that is in the DHS tool.

Mr. PITTS. Thank you, Mr. Chairman.

Mr. SHIMKUS. Thank you.

The chair now recognizes the gentleman from California, Mr. McNerney, for 5 minutes.

Mr. MCNERNEY. Thank you, Mr. Chairman.

Mr. Caldwell, we have been hearing this morning a lot about tiering formulas and about the risk assessment models. How familiar are you with the details of these models and formulas?

Mr. CALDWELL. We have not done the kind of verification and validation that a peer review of experts might do. So we have talked through what they use, we have discussed the factors, but I can't say we have tried to reproduce their models or do sensitivity analysis.

Mr. MCNERNEY. Are these by-and-large Excel spreadsheets or what do they look like? What form do they take or how do people have access to the models?

Mr. CALDWELL. It is an online tool so it is some kind of relational database. But beyond that, I can't tell you too much about the formulas or what the actual algorithms are.

Mr. MCNERNEY. And what sort of security do the models have in terms of making changes to parameters—not parameters but the way the models are executed? Is there a very secure methodology that is required for someone within DHS to change the model itself?

Mr. CALDWELL. We have not looked at the internal controls or the security settings on the model.

Mr. MCNERNEY. So as far as you know somebody in one of these departments can say, well, gee, I think this model is a little off; I am going to change it? I mean, there has to be some sort of control on these things.

Mr. CALDWELL. There should be, yes, sir.

Mr. MCNERNEY. Is that something you think you can find out or make an assessment?

Mr. CALDWELL. We can certainly ask the Department and answer that as a question for the record or if you could direct it to the Department, then that might expedite things or not.

Mr. MCNERNEY. All right. Thank you. I have a question. Were you assured by the under secretary's declaration that they have the best teams on cybersecurity and that they are on top of this issue and we don't have anything to worry about?

Mr. CALDWELL. That is not an aspect we looked at. So I have no comments on that.

Mr. MCNERNEY. So cybersecurity is not within your, sort of, realm?

Mr. CALDWELL. It is one of the many standards that they apply here. We do have other experts in GAO on cybersecurity that if you want to ask us a question for the record, we might be able to take that and answer it for you, sir.

Mr. MCNERNEY. All right. Thank you.

That is all I have, Mr. Chairman.

Mr. SHIMKUS. The chair thanks the gentleman.

The chair now recognizes, I believe, the gentleman from Ohio, Mr. Latta, for 5 minutes.

Mr. LATTA. Well, thank you very much, Mr. Chairman. And thank you very much for being here. And we have got a couple of hearings going on so I am sorry that we are kind of in out today.

But if I could start with this question: how important is it for the Infrastructure Security Compliance Division to have a complete validated and verified risk assessment approach?

Mr. CALDWELL. I mean I think our position is that the current approach is incomplete. So to the extent that they are using an incomplete model, they don't have an assurance that they are tiering these in the right fashion appropriate with the National Infrastructure Protection Plans criteria, which is, pretty much the Department's criteria in terms of how you do risk assessments.

Mr. LATTA. So how would you have to go about to get that complete?

Mr. WULF. You would have to include vulnerability in it and economic consequences are maybe the two minimum things that would need to be added into it. We have also asked that they update some of their threat data. Some of the threat data that they were using was a few years old, which they have agreed to do.

Mr. LATTA. OK. Thank you. Also, how important is it for the ISCD to eventually conduct an independent peer-review on CFATS risk assessment approach?

Mr. CALDWELL. We think it is very critical that there be an independent peer review. And I think you might have missed my answer talking to the chairman a few minutes ago, but there are really two factors. One is to make sure they have the methodology right, and secondly, to make sure the model, once you have the methodology right or at least with existing methodology, is the model actually functioning as intended? And as we have noted, there has been some miscalculations in the model that have been found which should, again, call for doing a verification and validation of the model itself.

Mr. LATTA. And just to follow up on that, how soon should that independent peer review occur?

Mr. CALDWELL. Well, I think it has already started. At least the panel that they have now, I think that there is a statement in Mr. Beers' written comments that if they need to do a second one, they are willing to do that as well. So the first one may be to find out where they are now, make some recommendations, and maybe would require a second peer review to actually go in and validate the model——

Mr. LATTA. OK.

Mr. CALDWELL [continuing]. With any changes.

Mr. LATTA. OK. Mr. Chairman, I have no further questions. Thank you.

Mr. SHIMKUS. And the chair thanks the gentleman.

The chair now recognizes the gentleman from Florida, Mr. Bilirakis, for 5 minutes.

Mr. BILIRAKIS. Thank you, Mr. Chairman. I appreciate it very much. I have one question. What is the difference between the current Site Security Plans and Alternative Security Plans?

Mr. CALDWELL. The Alternative Security Plans are written more like a plan. The Site Security Plans that DHS has I would describe as more of a data dump. It is a lot of different data that is in there. I mean, both can be useful, but I think industry feels—and you can ask the third panel—that the alternative site plan or the Alternative Security Plan is a little more user-friendly and still get you there in the end.

Mr. BILIRAKIS. Thank you, Mr. Chairman.

Mr. SHIMKUS. Seeing no other members present, we would like to thank you, Mr. Caldwell, for appearing before us. You have done great work on this report. It looks like we have got a lot more work to do.

And with that, we will allow the second panel to be dismissed and ask the third panel to join us at the table. Thank you, sir.

Mr. CALDWELL. Thank you very much.

Mr. SHIMKUS. We want to thank the third panel for joining us and sitting through most of the testimony. I am sure that is going

to be helpful for the remaining members as we listened to your opening statements and direct questions. And we will do so now.

The first person that I would like to recognize is—yes, I am going to recognize Mr. Allmond—that is oK, Jerry, I am great—Mr. Allmond, who is vice president of the Society of Chemical Manufactures and Affiliates. Sir, you are recognized for 5 minutes. Your full statement is in the record.

STATEMENTS OF BILL ALLMOND, VICE PRESIDENT, SOCIETY OF CHEMICAL MANUFACTURERS AND AFFILIATES; TIMOTHY J. SCOTT, CHIEF SECURITY OFFICER AND CORPORATE DIRECTOR, THE DOW CHEMICAL COMPANY, ON BEHALF OF THE AMERICAN CHEMISTRY COUNCIL; CHARLIE DREVNA, PRESIDENT, AMERICAN FUEL AND PETROCHEMICAL MANUFACTURERS; AND RICK HIND, LEGISLATIVE DIRECTOR, GREENPEACE

STATEMENT OF BILL ALLMOND

Mr. ALLMOND. Thank you. And good morning, Chairman Shimkus, Ranking Member Tonko, and members of the subcommittee.

My name is Bill Allmond and I am the vice president of Government and Public Relations at the Society of Chemical Manufacturers and Affiliates. I am pleased to have the opportunity to provide you with an update on the Department of Homeland Security's implementation of CFATS from the perspective of specialty chemical manufacturers, many of which are small and medium-sized companies.

Since the previous hearing last September, there are several areas we feel are worthy to highlight in terms of implementation progress. First, CFATS continues to reduce risk. Second, authorizing inspections are revealing some positives about DHS' implementation but also some challenges for small and medium-sized facilities. Lastly, a collaboration with the regulated community has improved.

With respect to risk reduction, CFATS continues to drive facilities to reduce inherent hazards where, in their judgment, doing so is in fact safer, does not transfer risk to some other point in the supply chain, and makes economic sense. Today, nearly 3,000 facilities have changed processes or inventories in ways that have enabled them to screen out of the regulation.

Furthermore, due to the outstanding cooperation of the chemical sector, there has been 100 percent compliance with requirements to date. DHS has not yet had to institute a single administrative penalty action to enforce compliance. As a result of CFATS, our Nation is more secure from terrorist chemical attacks than it was before the regulation's inception.

Turning to DHS' inspection process, the few that so far have been conducted at SOCMA members reveal some positive aspects about how the Department is carrying out the regulation, as well as some challenges being presented among small and medium-sized facilities. Among the positives is the level of interaction of DHS inspectors with facilities scheduled for an inspection. Inspectors are providing sufficient details with facilities prior to their arrival,

which aids the planning process to ensure resources and facility personnel are available.

Similarly, facilities are finding DHS inspectors generally to be reasonable during the onsite inspection, which is perhaps due to the fact that some of them have chemical facility experience. Such operational familiarity is necessary when interpreting how risk-based performance standards apply to, and could be implemented at, such facilities.

Importantly, inspections have so far appropriately verified a facility's approach to addressing risk-based performance standards. Inspectors appear not to be adhering rigidly to the RBPS guidance and instead to permitting company personnel to explain from the facility perspective, how they are appropriately implementing their Site Security Plan.

The principal challenge that SOCMA's smaller facilities are finding with the inspection process, however, is the enormous amount of time and resources to meet DHS demands following an inspection. Of highest concern is an unwillingness by DHS to reasonably extend deadlines for facility response. In SOCMA's opinion, DHS should be more willing to extend the time of which a small and medium-sized facility has to respond to a post-inspection report.

Facilities are learning that, even if they had an inspection that went well, they are having to rewrite much of their Site Security Plans. Under a 30-day deadline, which has been the usual case, facilities are having to pull two to three workers for 2 to 3 days each to ensure that they meet the deadline. To us, this is unreasonable. In small companies, there simply may not be more than a few people qualified to work on security measures and all those people have other obligations which frequently include compliance with other regulatory programs.

It is still early in the inspections process, and these burdens are now coming to light. However, DHS still has time to make adjustments given a willingness to do so.

And lastly, collaboration with facilities on implementation has improved. We are pleased that DHS has recently worked with industry to establish an alternative security program template with possibly more the future.

Additionally, DHS appears prepared this year to co-host another Chemical Sector Security Summit. For the past 6 years the Summit has been a collaborative effort by the Department and the chemical sector to provide an educational forum for CFATS stakeholders. An overwhelming majority of attendees each year are industry personnel who, when satisfaction surveys, consistently rate the Summit as having a high value to them.

Many of the improvements over the past year have occurred under leadership of Deputy Under Secretary Suzanne Spaulding and Director David Wulf and their actions to help put CFATS back on track is worthy of recognition. I appreciate the opportunity to testify this morning and I look forward to your questions.

[The prepared statement of Mr. Allmond follows:]

Testimony of

William E. Allmond, IV
Vice President, Government & Public Relations

Society of Chemical Manufacturers and Affiliates

before the

House Committee on Energy and Commerce
Subcommittee on Environment and the Economy

on

The Chemical Facility Anti-Terrorism Standards Program – A Progress Report

March 14, 2013

Good morning Chairman Shimkus, Ranking Member Tonko, and members of the Subcommittee. My name is Bill Allmond and I am Vice President of Government & Public Relations at the Society of Chemical Manufacturers and Affiliates (SOCMA). I am pleased to have the opportunity to provide you with a progress report on the Department of Homeland Security's implementation of its Chemical Facility Anti-Terrorism Standards (CFATS) from the perspective of specialty chemical manufacturers, many of which are small and medium-sized companies.

For 91 years, SOCMA has been and continues to be the leading trade association representing the specialty chemical industry. SOCMA's 200 member companies employ more than 100,000 workers across the country and produce some 50,000 products – valued at $60 billion annually – that make our standard of living possible. From pharmaceuticals to cosmetics, soaps to plastics and all manner of industrial and construction products, SOCMA members make materials that save lives, make our food supply safe and abundant, and enable the manufacture of literally thousands of other products. Over 80% of SOCMA's active members are small businesses.

Maintaining the security of our facilities has always been a priority for SOCMA members, and was so before September 11, 2001. After the tragic events of 9/11, SOCMA members did not wait for new government regulations before researching, investing in and implementing additional and far-reaching facility security measures to address these new threats. Under SOCMA's ChemStewards® initiative, SOCMA members were required to conduct security vulnerability assessments (SVAs) and to implement security measures. However, there were no uniform federal standards for measuring and implementing these security improvements across industry. CFATS standardized that security process.

Many SOCMA member company facilities are encompassed within the CFATS program. They have submitted their Site Security Plans (SSPs) and some are beginning to be inspected by DHS to verify the adequacy of those plans and their conformance to them. SOCMA members have spent an enormous amount of money and have devoted countless man-hours to secure their facilities and operations. These investments will naturally continue for the foreseeable future.

Definitively, DHS's Chemical Facility Anti-Terrorism Standards work. DHS listened to the private sector in developing a regulatory framework that is performance-based and preserves the ability for security professionals to make investments in measures that suit their specific facilities, but that also provides robust performance standards and imposes strict penalties for non-compliance.

But that does not mean that the CFATS experience has been easy for regulated companies, especially small and medium-sized facilities. Completing site security plans – and now, preparing for, participating in, and following up on inspections – requires substantial company resources and personnel.

I am pleased to report that there has been marked improvement in CFATS implementation under the leadership of National Programs and Protection Directorate (NPPD) Deputy Undersecretary Suzanne Spaulding and Infrastructure Security Compliance Division (ISCD) Director David Wulf, both of whom joined the Department in 2011. We also were encouraged by the

appointment of Scott Breor as Mr. Wolf's deputy. We are confident that this program will continue to move forward with these individuals at the helm.

Below I will (i) explain what is good about CFATS; (ii) describe lessons we are learning about the CFATS inspections process; and (iii) describe DHS' continued collaboration with industry.

I. CFATS is Reducing Risk

To be clear, SOCMA's membership regards the program thus far as a success, even if its implementation has moved much more slowly and cautiously than we all would prefer. The CFATS statute was wisely drafted to be comprehensive and flexibly structured to impose security performance standards that are relatively more demanding of higher-risk facilities and less demanding of lower-risk plants. To a great extent, DHS's rules implement the statutory mandate issued by Congress in 2006.

Both the law and the rules are fundamentally sound and do not require replacement. Since the program was launched in 2007, more than 2,000 facilities have changed processes or inventories in ways that have enabled them to screen out of the program. Thus, as predicted, CFATS is driving facilities to reduce inherent hazards, where in their expert judgment doing so is in fact safer, does not transfer risk to some other point in the supply chain, and makes economic sense. Hundreds of other regulated facilities that had not already done so have already made significant proactive investments in security measures in anticipation of compliance with the full implementation of CFATS. As a result of CFATS, our nation is more secure from terrorist chemical attacks and other threats than it was before the program's inception. And this risk reduction has taken place through a market-based approach that has certainly cost society less than if all the initially covered facilities were still subject to regulation.

Furthermore, due to the outstanding cooperation of the chemical sector, there has been 100% compliance with the requirements to submit Top-Screens, SVAs and SSPs – DHS has not yet had to institute a single administrative penalty action to enforce compliance.

SOCMA also supports the CFATS program because our members have invested significant amounts of financial and human capital in it over the past several years. SOCMA's members alone, a majority of which are small manufacturers with under $40 million in annual sales, have invested an estimated $515 million in security measures to date. CFATS has provided significant additional security to a critical segment of our nation's infrastructure, as well as the general public.

No one should dispute that, despite challenges to its implementation, the two main alternatives to CFATS would both be far worse. Having no chemical security regulation at all would create a risky and tilted playing field in which most companies secured their facilities voluntarily, at significant cost, while a minority created risks for us all, and gained an unfair economic advantage, by not doing so. Our nation would also not be well-served by a prescriptive program that mandated incorporation of inherently safer technology (IST). Such an approach would threaten to drive chemical operations overseas where security standards are weaker.

II. Inspections Reveal Positives, Challenges for Small & Medium-Sized Facilities

A. Communication by Inspectors Appears to Be Positive

From the few inspections that have so far been conducted of SOCMA members, the interaction of DHS inspectors with facilities scheduled for an inspection appears to be positive. Inspectors are providing sufficient details with facilities prior to their arrival onsite, including an itinerary for their visit, which greatly assists facility personnel in planning ahead for the inspector to ensure resources and personnel are available if needed.

This is not altogether surprising, however. Regional commanders and inspectors have regularly made themselves available to SOCMA over the past several years. As we testified to this Subcommittee last September, DHS inspectors have repeatedly provided compliance assistance onsite upon request or participated in SOCMA events, engaging with our membership. Many of them also attend the Chemical Sector Security Summit each year, which SOCMA co-funds with DHS.

This level of communication may not be true of all DHS CFATS inspectors, but it is what we have learned from facilities with which we have spoken and what we at the organization have witnessed.

B. On-Site Inspection Process So Far Appears to Be Reasonably Executed

Facilities are finding DHS inspectors generally to be reasonable during the onsite inspection. Among the personnel conducting the inspections are individuals with chemical industry experience, which is critical when interpreting how risk-based performance standards apply to and could be implemented at chemical manufacturing facilities.

The amount of time spent by inspectors on-site conducting the facility is also, thus far, reasonable. Some facilities are reporting that their facility inspection took two to three days, less than the amount of time once generally assumed based on the first reports.

Importantly, inspections of which we are aware have appropriately verified a facility's approach to addressing applicable Risk Based Performance Standards (RBPS). Inspectors appear not to be adhering rigidly to the RBPS Guidance and, instead, to be permitting company personnel to explain, from the facility perspective, how they are appropriately implementing their site security plan.

C. Inspections Are Requiring an Enormous Amount of Facility Time and Personnel

The principal challenge that SOCMA's small and medium-sized chemical facilities are finding with the inspection process is the enormous amount of time and resources to prepare for an inspection and, in particular, to respond to one after it has been completed.

SOCMA members are familiar with onsite inspections. Due to their required adherence to other regulations, many of our members are regularly inspected by various government agencies,

including the Environmental Protection Agency, the Food and Drug Administration, and the Occupational Safety and Health Administration – to name just several. Additionally, every manufacturing facility that our members operate must undergo periodic third party verification mandated by SOCMA's ChemStewards® program. With CFATS, however, our members have encountered so far an unwillingness to reasonably extend deadlines or provide additional time for facility response.

DHS should be more willing to extend the amount of time a small and medium-sized facility has to respond to a post-inspection report. Facilities are learning that, even if they had an inspection that overall seemed to go well, they are having to rewrite much of their site security plan to address issues discovered during the inspection. It is difficult for these smaller facilities to mobilize sufficient personnel to address such requirements following a CFATS inspection within a deadline of 30 days, which has been the usual case. Under a 30-day deadline, facilities are having to pull two to three workers for two to three days each—a total of over 70 man hours—from their productive jobs to ensure they meet the deadline. To us, this is unreasonable. Larger companies have more qualified personnel available to be redirected in such ways. In small companies, however, there simply may not be more than a few people qualified to work on security measures. And all of those people have other obligations, which frequently include compliance with other regulatory programs.

Highlighting our desire for more flexibility with deadlines, the Manufacturers Alliance for Productivity and Innovation released a study[1] last fall that found that chemical manufacturing output could fall 9%-10% per year on average over the next decade because of the cost of federal regulations. Given this prospect, we welcome as much flexibility as can reasonably be allowed by federal agencies during regulatory implementation.

Because their ability to continue selling products in the marketplace generally requires successful performance on inspections, SOCMA members place a high priority on preparing for and performing well on these inspections. We don't question DHS's need for additional information following an inspection; like other inspections, it is most often an expected part of the process. Nevertheless, given our members' small size and the enormously challenging deadlines they are under, it seems reasonable to us for DHS to give them more time to respond to inspections. It is still early in the inspections process and these burdens are now coming to light among SOCMA's members. DHS still has time to make adjustments and we are confident that, following today's hearing, they will consider our perspective.

III. Collaboration with the Regulated Community on Implementation Has Improved

As SOCMA has previously testified, the CFATS framework is sound. We have cautioned that, while the standards are sound, ISCD should work collaboratively with the regulated community to solve the technical, training and tool-related issues currently presenting challenges to CFATS implementation. We are pleased that DHS has worked closely with industry to establish an Alternative Security Program template. This development is certainly a public commitment by

[1] Manufacturers Alliance for Productivity and Innovation, *Macroeconomic Impacts of Federal Regulation of the Manufacturing Sector* (August 21, 2012) at 9, available at http://www.mapi.net/research/publications/macroeconomic-impacts-federal-regulation-manufacturing-sector.

DHS to better collaborate on implementation.

Additionally, DHS appears prepared to co-host another Chemical Sector Security Summit this year. The summit is a collaborative effort by the Department and the Chemical Sector Coordinating Council to provide a public educational forum for CFATS stakeholders. An overwhelming majority of attendees each year are industry representatives. SOCMA members, in particular, find high value in this collaborative event. We fully expect that DHS will again work with us to provide this opportunity this year.

IV. Conclusion

SOCMA believes that DHS has steadily improved its implementation of CFATS in recent months. However, the inspections process is showing mixed results; while it is generally working well, DHS needs to show more flexibility in setting deadlines for small and medium-sized facilities.

I appreciate this opportunity to testify before you today and look forward to your questions.

Mr. SHIMKUS. Thank you very much. I would now like to recognize, as I move my papers all around—where is his name? Here it is—Mr. Timothy Scott, Chief Security Officer and Corporate Director of Dow Chemical Company, on behalf of The American Chemistry Council. Sir, you are recognized for 5 minutes.

STATEMENT OF TIMOTHY J. SCOTT

Mr. SCOTT. Thank you, Chairman Shimkus, Ranking Member Tonko, and members of the subcommittee. I am Tim Scott, Chief Security officer of the Dow Chemical Company, speaking today on behalf of Dow and the American Chemistry Counsel.

The chemical industry and Department of Homeland Security have a common goal: to improve the security profile of the chemical sector and reduce the risk of attack against industry or the use of chemicals as a weapon. Our positions are that security is a top priority of the chemical industry. Progress has been made in all areas of chemical security, but there is still, obviously, work to be done. ACC will continue to partner with DHS to achieve success and we need the certainty of a multiyear extension of DHS authority for a sustainable program. Progress has been made and we need to build on that progress as respectful partners with different skills and expertise but with a common goal.

DHS has evaluated nearly 40,000 chemical facilities across United States initially identifying more than 7,000 as potentially high-risk. Since then, more than 3,000 facilities have lowered their chemical risk profile, clear evidence that we have made progress. Last year, ACC published an alternative security program guidance document available at no cost to the regulated community, the result of a year-long effort and full cooperation with DHS. This ASP approach offers an efficient alternative to DHS process and is an excellent example of how an effective public-private partnership can create smart regulatory solutions that benefit both partners, while ensuring the security and safety of our industry.

While we have made progress, there are many more opportunities for efficient and effective compliance options that will accelerate CFATS implementation while maintaining the quality and integrity of the program. Existing industry security programs such as the Responsible Care Security Code should be recognized by DHS under their ASP authority as meeting the initial hurdles for authorization, thus streamlining and prioritizing reviews, especially at the lower tiered sites.

We must develop a workable process regarding personnel surety. The goal of the PSP program is to ensure that personnel accessing sensitive sites of high-risk chemical facilities are trustworthy and do not pose a security risk. It is essential that these individuals are properly vetted against the terrorist screening database. We all agree on that. But is also essential that the site know these individuals are cleared before granting access to such sensitive areas.

Under the current proposals, industry submits the individual's personal information and receives no verification of any kind. We are supposed to be satisfied that simply submitting the data is enough to grant site access. This is simply a poor security practice, especially when solutions already exist. It is good to hear that we may be making progress in this area with DHS. By leveraging ex-

isting PSP programs and allowing for corporate and third-party submissions for vetting against a terrorist screening database, a significant reporting burden will be minimized and the integrity of the program will be much improved.

Another opportunity for efficiency that can easily be implemented is in what we call corporate audits. These audits cover areas of the risk-based performance standards in which many companies' sites operate under a single corporate process, such as cybersecurity or security escalation processes. Current inspections often have inspectors getting the same corporate answers site-by-site instead of addressing the issue once at the corporate level. This can unnecessarily extend the length of a site inspection. We also heard that DHS is working on this.

ACC believes that DHS should be more transparent about all factors related to a covered facility's risk assessment. Trust is at the core of an effective security partnership and ACC strongly recommends that DHS improve the transparency of its risk determinations with the site security managers. A lack of transparency has been the source for many of the inefficiencies and missteps during the CFATS implementation.

The CFATS concept is fundamentally sound, risk-based, focused on the right priorities allowing regulated sites to choose and apply customized security solutions for DHS review and evaluation for compliance with the DHS-established risk-based performance standards. And that is the goal, to meet the standards. And industry will.

DHS has demonstrated renewed commitment and effort to our partnership due in part by oversight of this committee. ACC urges Congress to provide DHS extended statutory authority for the CFATS program to provide the regulatory certainty and stability needed for industry to make prudent security investment and capital planning decisions. Industry and DHS have made progress in improving the security of the chemical sector. There have been missteps, but we should acknowledge the progress and the challenge and commit to making CFATS work. Thank you.

[The prepared statement of Mr. Scott follows:]

Written Statement of

Timothy J. Scott
Chief Security Officer and Corporate Director
Emergency Services and Security
The Dow Chemical Company

Representing

The American Chemistry Council

To the

United States House of Representatives
Subcommittee on Environment and the Economy

On

"The Chemical Facility Anti-Terrorism Standards (CFATS) Program: A Progress Update."

Oversight Hearing on Thursday, March 14, 2013
10:00 a.m., 2322 Rayburn

Security Is a Top Priority for the Chemical Industry

The American Chemistry Council (ACC) represents the leading chemical companies that produce essential products critical to everyday life. The business of chemistry is a critical aspect of our nation's economy since it employs more than 780,000 Americans and touches more than 96 percent of all manufactured goods.

Because of our critical role in the economy, our commitment to our customers and shareholders and our responsibility to our neighboring communities, safety and security remain a top priority. In 2001, ACC members adopted an aggressive voluntary security program, the Responsible Care® Security Code (RCSC). RCSC is a comprehensive program that covers physical and cybersecurity vulnerabilities and requires ACC members to perform a thorough assessment of its security risks, to identify vulnerabilities and to implement appropriate protective measures throughout their value chain. Responsible Care implementation is mandatory for all ACC members, and its implementation is verified by independent, credentialed third-party auditors.

The RCSC has been a model for state-level chemical security programs in New Jersey, New York and Maryland, and the U. S. Coast Guard recognized it as an approved alternative security plan for compliance with the Maritime Transportation Security Act (MTSA). To date, ACC members have invested over $11 billion in security enhancements under the auspices of the RCSC and in compliance with MTSA and CFATS regulatory programs.

DHS and Industry Have Made Significant Strides to Enhance Chemical Security

ACC believes that CFATS has had a positive impact on enhancing security, and we support full implementation of the program. Under CFATS, the Department of Homeland Security (DHS) has analyzed nearly 40,000 chemical facilities across the United States, identifying more than 7,000 facilities as potentially high-risk chemical facilities. Since then nearly 3,000 facilities have lowered their potential security risks by making operational changes that reduced or eliminated onsite chemical inventories. As a result, the CFATS regulated community currently includes approximately 4,500 facilities across the nation.

While DHS has faced some challenges implementing the CFATS program, these challenges are not insurmountable. Since the release of the DHS internal memo, the agency has made progress on implementing the action items and putting in place a workable management structure that will enable an effective CFATS implementation process. The industry has seen considerably increased inspection activity, improved quality of inspections and expedited authorizations. Key management positions have been filled with permanent, qualified professionals who have regulatory program experience. DHS has reengaged the public/private sector security partnership that was so valuable early in the program and is now providing an opportunity to make additional strides as we work together in securing the nation's chemical infrastructure.

Alternative Security Programs Offer a Valuable Opportunity

In December 2012, ACC published the Alternative Security Program (ASP) Guidance Document and Template, which are available to the regulated community for free on our website at: http://www.americanchemistry.com/Policy/Security. This initiative was the result of a yearlong effort in cooperation with DHS aimed at providing a set of compliance guidelines for the CFATS community on

developing an effective ASP. The ASP Guidance Document and Template provides helpful guidance on how to create an effective security plan for submission to DHS that clearly demonstrates a facility's compliance with the 18 Risk Based Performance Standards (RBPS), while providing an operational plan that can be used by site security personnel as well as DHS inspectors during an audit. This ASP approach offers an effective alternative to the existing Sector-Specific Plans (SSP) process, which has been identified as one of the significant roadblocks in moving CFATS approvals forward.

In a letter from David Wulf, DHS Director of the Infrastructure Security Compliance Division, he commends the work of ACC and our members in developing this important document and our decision to make them broadly available to the regulated community. Further, DHS states, "ASPs will undoubtedly be an important part of the CFATS program's continued forward progress."

The ASP initiative is an excellent example of how an effective public/private security partnership can create smart regulatory solutions that will benefit both the regulated community and DHS, while ensuring the security and safety of our infrastructure, our workers and our communities.

While DHS has made progress in moving the CFATS program forward, more needs to be done. DHS's authority to accept ASPs is an opportunity to expand on this initial work and develop effective compliance options that will help accelerate CFATS implementation, while ensuring the quality of the program. Existing industry security programs, such as the RCSC, should be recognized by DHS under their ASP authority as meeting initial hurdles for authorization, thus streamlining and prioritizing reviews. Industry sector ASPs could be created and approved by DHS and would cover a broad swath of the CFATS-regulated community, thus improving efficiency and expediting approvals. Clearly, given the future challenges facing DHS, particularly with processing the mountain of lower-tier sites, we need to develop innovative solutions to ensure chemical security across the country in a timely fashion.

Lastly, another opportunity for efficiency that could easily be implemented is the "corporate audit." Corporate audits cover those risk-based performance standards in which many facilities operate under a single corporate procedure or set of guidelines. Cybersecurity and site security escalation processes are two common examples. Current CFATS inspections often have inspectors getting the same corporate answer, site-by-site, instead addressing the issue once, unnecessarily expanding the length of a site inspection and the associated resources.

DHS Should Expedite an Effective Personnel Surety Program

Since DHS withdrew its personnel surety proposal from the Office of Management and Budget (OMB) this past summer, DHS has done a commendable job in reaching out to stakeholders and incorporating many of their ideas to help streamline the proposal and reduce the burden on the regulated community. By leveraging existing programs, such as the Transportation Worker Identification Credential (TWIC), and by allowing for corporate and third-party submissions for vetting against the Terrorist Screening Database (TSDB), a significant reporting burden will be minimized while maintaining the integrity of the program.

However, despite this progress, DHS does not currently have a workable Personnel Surety Program (PSP) program in place, resulting in no security plans being completely authorized or approved. This deficiency is a significant issue that must be addressed to ensure that all high-risk chemical facilities are safe, secure and fully comply with CFATS.

The goal of PSP is to ensure that personnel who have access to sensitive areas of high-risk chemical facilities are trustworthy and do not pose a security risk to the facility, to its workers or to members of the surrounding community. However, the current PSP proposal does not provide appropriate personnel assurance since DHS does not provide adequate notification to the facility that a person has been properly cleared prior to their entry to sensitive areas within a covered facility. This approach is counter to the core mission of the CFATS program and could needlessly put a facility and the surrounding community at risk. It is crucial, therefore, that such personnel are properly evaluated against the TSDB and are cleared *prior* to being granted access to such sensitive areas. Therefore, DHS must provide proper and timely notification to the facility that such persons have been assessed and are cleared for access *prior* to entry.

The CFATS Program Would Greatly Benefit from Improved Transparency

Each CFATS-covered facility receives a risk-based tier designation that is based on an analysis of the type and quantities of CFATS covered chemicals, or Chemicals of Interest (COI), and potential security risks such as theft or intentional release. In its final tiering determination letter, each facility is given a tier ranking between 1 through 4, with Tier 1 being the highest risk and Tier 4 being the lowest risk associated with its COI and potential security issues. However, other tiering factors such as local threat information are not shared with the facility. In some cases, some ACC members have questioned their tier assignment either because it does not mesh with the onsite security assessment or it is inconsistent with other similar covered facilities managed by the same company. However, when engaging DHS on their tier assignment, the typical response is that it is "classified."

ACC believes that DHS should be more transparent about all factors related to a covered facility's risk-based tiering, even if it needs to be at the classified level. The security manager at the site has the ultimate responsibility for the safety and security of its operations, and he or she also has the authority to make informed risk mitigation and security investment decisions. ACC believes that this issue is at the core of an effective security partnership. ACC strongly recommends that DHS improve the transparency of its risk-based tier determinations with the local security managers, by request, even if it has to be in a classified setting.

ACC Supports the CFATS Regulatory Program

DHS has created a solid regulatory framework under CFATS. This comprehensive federal regulatory program requires high-risk chemical facilities to register with DHS (Top Screen), conduct a thorough site security assessment and implement protective measures that comply with 18 risk based performance standards. These standards provide a solid, technical foundation for addressing a covered facility's security measures such as perimeter security, access control, personnel surety and cybersecurity. To meet the RBPS, covered facilities select from an array of security risk reduction measures that are appropriate for their site-specific circumstances and achieve the requisite level of performance. DHS inspectors conduct thorough site assessments and work with the facility to ensure security and compliance with regulatory requirements. For ACC members, this assessment is exactly what a strong regulatory approach must do - ***set a high bar through performance-based standards and then hold facilities accountable.*** The CFATS approach allows facilities to utilize a full range of potential security enhancements depending on local site conditions and risk thus maximizing their potential effectiveness.

Congress Should Continue to Support the CFATS Program

DHS leadership has demonstrated a commitment to working through the current issues and working with stakeholders to improve the implementation of the CFATS program. ACC urges Congress to provide the agency with sufficient resources to properly handle the workload and to ensure that chemical facility security is implemented in a timely fashion. Eventually we hope that Congress will provide DHS permanent statutory authority for the CFATS program, thus providing regulatory certainty and operational stability that is necessary for capital investments to be appropriately planned and budgeted. These improvements will also ensure that long-term security decisions can be made without concern as to whether the regulatory landscape under the CFATS program will be altered.

Mr. SHIMKUS. Thank you. Next, I would like to recognize Mr. Charlie Drevna, President, American Fuel and Petrochemical Manufacturers.

Sir, you are recognized for 5 minutes.

STATEMENT OF CHARLIE DREVNA

Mr. DREVNA. Chairman Shimkus, Ranking Member Tonko, and members of the subcommittee, thank you for giving me the opportunity to testify today on today's hearing on the progress report of the CFATS program. I am Charlie Drevna and I serve as president of AFPM.

We are a 111-year-old trade association representing high-tech American manufactures that use oil and natural gas liquids as raw materials to make virtually the entire supply of U.S. gasoline, diesel, jet fuel, other fuels such as home heating oil, as well as the petrochemicals used as building blocks for thousands of products vital in everyone's daily lives.

America's refining and petrochemical companies play a pivotal role in ensuring and maintaining the security of America's energy and petrochemical infrastructure. Nothing is more important to AFPM member companies than the safety and security of our employees, facilities, and communities. Our members have worked extensively with the Department of Homeland Security and we have invested hundreds of millions of dollars. And we don't mind investing the money as long as we know it is going for the right reasons, and again, toward strengthening facility security.

Our industry also recognizes that protection of critical infrastructure against potential threats or terrorist attacks should be a shared responsibility between government and stakeholders.

AFPM appreciates that DHS conducted an internal review to identify administrative and implementation problems that require immediate action and that the Agency developed an Action Plan for improving CFATS implementation. But it is important, however, to recognize that the structure of the CFATS framework itself is sound, even though the leaked report from GAO revealed the implementation of CFATS program was somewhat flawed.

Additionally, America's critical infrastructure facilities are secure and there have been no attacks on chemical facilities since development of the CFATS program. Nonetheless, it is clear that DHS needs to better manage its resources and set priorities to make progress in areas that need immediate action, including faster approval of Site Security Plans and finalizing a workable Personnel Surety Program, a PSP. Such measures would work to strengthen the program and our national security.

AFPM believes that DHS has made progress over the past year to address the problems identified in the DHS-leaked report and Action Plan. However, DHS should continue to make improvements by addressing issues including personnel surety with the help of the industry in order to enhance the overall effectiveness of CFATS implementation in the short-term.

AFPM is pleased that DHS withdrew the personnel surety proposal from the Office of Management and Budget last July and then held a series of meetings with industry to take another look at this issue. Congress intended, and I heard today a repeat of that

intent, that the risk-based performance standard on personnel surety which governs access to high-risk facilities, allow facilities the flexibility to determine the most efficient manner to meet that standard.

Instead, DHS initially proposed and arguably prescribed PSP program that failed to recognize the Transportation Worker Identification Credential, or TWIC card, and other established federal vetting programs. Such a program would have been burdensome to both DHS and industry, and would be a wasteful and ineffective use of agency and industry resources. Instead of proposing a duplicative, burdensome PSP, DHS should remain focused on fixing the current problems and not expand beyond the scopes of the core CFATS program.

The PSP program must be fixed soon and we hope that DHS will honor the TWIC and other federal credentials at CFATS sites. Facilities should have the option to use federally secure vetting programs such as TWIC to satisfy CFATS without submitting additional personnel information. AFPM supports a PSP program that requires only a one-time submission of personnel identifying information to DHS, recognition of TWIC and other federal credentials, and the use of third-party submitters for corporate submissions. This would lessen the burden on both DHS and industry, and would potentially account for half of the population affected by the Personnel Surety Programs, specifically, contractors coming to CFATS sites who would already have those cards.

Stakeholder input is necessary. To assist DHS in addressing CFATS implementation challenges, continued stakeholder input is necessary. We are encouraged that we are seeing DHS do this more and more.

In summary, AFPM believes that DHS has made progress over the year addressing the problems identified in the internal report. We also acknowledge that there is been far greater outreach and more detailed discussions with DHS, and we hope that those continue in the future.

Thank you and I look forward to any questions you may have regarding my testimony.

[The prepared statement of Mr. Drevna follows:]

WRITTEN STATEMENT OF THE

AMERICAN FUEL & PETROCHEMICAL MANUFACTURERS (AFPM)

AS SUBMITTED TO THE

SUBCOMMITTEE ON ENVIRONMENT AND THE ECONOMY

Committee on Energy and Commerce
United States House of Representatives

For a Hearing entitled,

"The Chemical Facility Anti-Terrorism Standards
(CFATS) Program – A Progress Update."

March 14, 2013

Testimony Summary of Charles Drevna, president of the American Fuel & Petrochemical Manufacturers (AFPM)

House Committee on Energy and Commerce – Subcommittee on Environment & the Economy, Hearing on "The Chemical Facility Anti-Terrorism Standards (CFATS) Program – A Progress Update."

America's refining and petrochemical companies play a pivotal role in ensuring and maintaining the security of America's energy and petrochemical infrastructure. Nothing is more important to AFPM's member companies than the safety and security of our employees, facilities and communities. Our members have worked extensively with the Department of Homeland Security (DHS) – and have invested millions of dollars – toward strengthening facility security. Our industry recognizes that protection of critical infrastructure against potential threats or terrorist attacks should be a shared responsibility between government and stakeholders.

AFPM appreciates that DHS conducted an internal review to identify administrative problems that need fixing immediately and that the agency developed an action plan for improving CFATS implementation. AFPM believes that DHS has made progress over the past year fixing the problems identified in the DHS leaked internal report.

It is important to recognize that the structure of the CFATS framework itself is sound. Nonetheless, it is clear that DHS needed to better manage its resources and set priorities to make progress in areas that need immediate attention, including faster approval of site security plans (SSPs) and finalizing a workable personnel surety program. Such measures would work to strengthen the program and our national security.

To assist DHS in addressing these CFATS implementation challenges, continued stakeholder input is needed. It is encouraging that since the internal report leaked, DHS has met with stakeholders much more than in recent years. Areas that industry and DHS continue to focus on include risk tier modeling, personnel surety and tool-related issues that were identified in the DHS internal review. DHS has also started taking steps to improve the approval process of SSPs and is reviewing risk tier modeling.

AFPM is pleased that DHS withdrew the Personnel Surety Proposal (PSP) from the Office of Management & Budget (OMB) and then held numerous meetings with industry to take another look at the personnel surety issue. AFPM remains hopeful that we can come to a workable solution soon on personnel surety and hopes that collaboration will yield a less burdensome, yet still protective PSP for CFATS sites. Additionally, as DHS works to resubmit a PSP proposal, it is important that any proposal follows Congressional intent and be written as a risk-based performance standard. The PSP program must be fixed soon and we hope that DHS will honor the Transportation Worker Identification Credential (TWIC) and other Federal credentials at CFATS sites. Facilities should have the option to use established federally secure vetting programs, such as the TWIC, to satisfy CFATS without submitting additional personnel information to DHS.

I. Introduction

Chairman Shimkus, Ranking Member Tonko and Members of the Subcommittee, thank you for providing the opportunity to testify at today's hearing on a progress report of the Chemical Facility Anti-Terrorism Standards (CFATS) program. I'm Charlie Drevna, and I serve as president of AFPM, the American Fuel & Petrochemical Manufacturers.

AFPM is a 111-year old trade association representing high-tech American manufacturers that use oil and natural gas liquids as raw materials to make virtually the entire U.S. supply of gasoline, diesel, jet fuel, other fuels and home heating oil, as well as the petrochemicals used as building blocks for thousands of vital products in daily life. AFPM members make modern life possible while keeping America moving and growing as we meet the needs of our nation and local communities, strengthen economic and national security, and support 2 million American jobs.

America's refining and petrochemical companies play a pivotal role in ensuring and maintaining the security of America's energy and petrochemical infrastructure. Nothing is more important to AFPM's member companies than the safety and security of our employees, facilities and communities. Our members have worked extensively with the Department of Homeland Security (DHS) – and have invested millions of dollars – toward strengthening facility security. Our industry recognizes that protection of critical infrastructure against potential threats or terrorist attacks should be a shared responsibility between government and stakeholders.

II. DHS and CFATS Program

AFPM appreciates that DHS conducted an internal review to identify administrative problems that need fixing immediately and that the agency developed an action plan for improving CFATS implementation. It is important to recognize that the structure of the CFATS framework itself is sound. Since the beginning of the CFATS program, DHS and industry, including some AFPM members, worked together and developed robust, risk-based performance standards (RBPS) that avoid being too prescriptive for an industry as diverse in size and function as the chemical sector, but that also include strict enforcement penalties for noncompliance. For example, each site develops a unique and appropriate Site Security Plan to address the specific risk issues of the facility, while meeting DHS-established risk-based performance standards. Since the inception of CFATS, facilities have proactively invested in security to comply with, and indeed exceed, requirements of the regulations.

Since the development of the CFATS program AFPM's members have also partnered with DHS on many important security initiatives and programs, including the Risk Assessment Methodology for Critical Asset Protection (RAMCAP), Site Vulnerability Assessments (SVAs), Site Security Plans (SSPs), and by our participation in the Chemical Sector Coordinating Council (CSCC) and the Oil and Natural Gas Sector Coordinating Council (ONGSCC).

America's critical infrastructure facilities are secure and there have been no terrorist attacks on chemical facilities since the development of the CFATS program. Nonetheless, it is clear that DHS needed to better manage its resources and set priorities to make progress in areas that need immediate attention, including faster approval of site security plans and finalizing a workable personnel surety program. Such measures would work to strengthen the program and our national security.

To assist DHS in addressing these CFATS implementation challenges, continued stakeholder input is needed. It is encouraging that since the internal report leaked, DHS has met with stakeholders much more than in recent years. Areas that industry and DHS continue to focus on include risk tier modeling, personnel surety and tool-related issues that were identified in the DHS internal review.

AFPM recognizes that there are internal personnel and financial issues within DHS that must be addressed administratively where industry has no role. However, DHS could continue to make improvements by addressing the following issues quickly, with the help of industry, in order to enhance the effectiveness of CFATS implementation in the short-term.

- **Personnel Surety Program (PSP)** – Congress intended that the Risk-Based Performance Standard 12 on Personnel Surety, which governs access to high-risk facilities, to allow facilities the flexibility to determine the most efficient manner to meet the standard. Instead, DHS ***initially*** proposed a personnel surety program that failed to recognize, and actually would have duplicated, already established federal vetting programs. Such a program would have been burdensome to both DHS and industry and would be a wasteful and ineffective use of agency and industry resources. DHS should remain focused on fixing the current problems and not expand beyond the scope of the core CFATS program.

  AFPM is encouraged and applauds DHS for withdrawing the PSP proposal from OMB in July 2012. Moreover, AFPM is pleased that DHS decided to hold a series of stakeholder meetings with industry to take another look at the personnel surety issue, and hopes that collaboration will yield a less burdensome, yet still protective PSP for CFATS sites. Additionally, as DHS works to resubmit a PSP proposal, it is important that any proposal follows Congressional intent and be written as a performance standard. The PSP program must be fixed soon and we hope that DHS will honor the Transportation Worker Identification Credential (TWIC) and other Federal credentials at CFATS sites. Facilities should have the option to use established federally secure vetting programs, such as the TWIC, to satisfy CFATS without submitting additional personnel information to DHS.

- **Site Security Plans** - DHS should focus on the Tier 1 Site Security Plan (SSP) approvals, as they are considered the highest risk sites and have had their SSPs submitted to DHS the longest. DHS is currently holding a series of outreach meetings around the country to

discuss with owners and operators how to improve the SSP. AFPM applauds recent efforts, however, as we suggested to DHS, we think it should have been done years ago.

DHS should also consider approving alternative security plans (ASPs) for a variety of CFATS sites. DHS should work with all sectors governed by CFATS to develop ASPs. For sites that are smaller or contain fewer chemicals of interest (COIs) an ASP makes sense and would result in review and approval time for ASPs not taking as long as for a regular SSP.

- **Inspections** - Inspections are a key part of the Site Security Plan approval process. Like SSPs, DHS should focus on Tier 1 sites. DHS recently started up CFATS inspector training courses and developed new inspection guidelines for inspectors. AFPM offered multiple times for DHS to have our members speak at the inspector training classes to provide an overview of the chemical and oil and natural gas industry and the CFATS applicability issues at those sites. To date, DHS has yet to take us up on this offer. AFPM believes this would be an invaluable opportunity for new inspectors to learn about security practices at CFATS sites prior to going to a site. AFPM hopes that DHS will consider this offer.

- **Risk Modeling**—AFPM is strongly concerned that the DHS risk modeling used for setting risk tier levels for facilities in CFATS is seriously flawed. AFPM continues to ask DHS to be more transparent regarding DHS risk modeling and risk tier level determinations.

  The risk modeling of the CFATS sites is the foundation of the CFATS program and AFPM is encouraged that DHS established a peer review panel to resolve the modeling issues. However—we again question why this was not done sooner as flaws in the risk modeling have been brought to DHS numerous times.

- **Stakeholder Input** - Stakeholder input is important for security awareness and creating the best plans to secure our critical infrastructure. The framework of the CFATS program is sound and was developed with industry's input. Securing the nation's critical infrastructure must be done with industry at the table or the unfortunate implementation issues the program has experienced to date could be repeated.

  Many of the implementation delays have resulted from the lack of knowledge and experience within DHS' Infrastructure Security Compliance Division (ISCD). For example, the Top Screen process did not work for many companies during the beginning of the CFATS program. In this instance, ISCD did not know that the oil and natural gas sector stores millions of pounds of materials, not thousands. The data field in the web page simply did not include enough digits to record actual volumes and required several weeks to correct. It is worth noting, however, that the level of stakeholder outreach has vastly improved in the past year. AFPM encourages DHS to continue this positive trend.

- **Transparency** - Informed discussions with stakeholders will lead to less confusion and quicken implementation for all parties. In particular, in the National Academies of

Science's (NAS) 2010 "Review of the Department of Homeland Security's Approach to Risk Analysis," the NAS comments multiple times on the significance of stakeholder involvement and transparency in effective risk modeling. While NAS is commenting on risk assessment practices within DHS, the comment is directly applicable to CFATS implementation. The NAS recommendations for transparency and stakeholder input would provide benefit not only for the risk assessment practices within the ISCD, but also provide substantial improvement on rule implementation.

III. Conclusion

In summary, AFPM believes that DHS has made progress over the past year fixing the problems identified in the DHS leaked internal report. AFPM acknowledges that there has been far greater outreach and much more detailed discussions by DHS with industry this past year than previously. DHS has also started taking steps to improve the approval process of site security plans and is reviewing the risk tier modeling. AFPM is pleased that DHS withdrew the Personnel Surety Proposal from OMB and then held numerous meetings with industry to take another look at the personnel surety issue. AFPM remains hopeful that we can come to a workable solution soon on personnel surety and hopes that collaboration will yield a less burdensome, yet still protective PSP for CFATS sites.

Thank you again for the opportunity to testify before the Committee today. I look forward to working with you as Congress continues oversight on the progress of CFATS implementation.

Mr. SHIMKUS. Thank you. And now the chair recognizes Mr. Rick Hind, Legislative Director for Greenpeace. Sir, you are recognized for 5 minutes.

STATEMENT OF RICK HIND

Mr. HIND. Thank you, Mr. Chairman. My name is Rick Hind. I am the legislative director of Greenpeace, as you mentioned. I appreciate the opportunity to talk to you today both to this committee and with this panel here.

We work with over 100 other organizations, mainly unions, environmental justice organizations, other environmental groups, security experts, 9/11 families, and others who, for 10 years, have pushed for disaster prevention. The legislation that passed the House in 2009—November, actually, 2009—had that component in it but it also addressed a lot of the problems that you have been hearing about today. It provided for regular scheduling of the DHS issuing vulnerability and security plans as well as keeping regular reports back to Congress. I think you probably would have been hearing about any these problems in 2011 at the latest if that legislation had been enacted in 2010.

That legislation also would have seamlessly replaced the 2006 authorization that you have referred to earlier, which was never really thought to be adequate. Everybody knew that and that is why it had a 3-year expiration date on it. And today, we are extending it now 6 years, 1 or so years at a time, and therefore, I think you have appropriately given the due that DHS staff deserved. Their dedication and stick-to-itiveness in a program that is really inadequate, from the legislative foundation through to the continuity of its funding by Congress.

However, the kind of big elephants in the room that we see unaddressed are the fact that the statute actually prohibits the government from requiring disaster prevention in the statute barring any particular security measure for approval of security plans. In addition, the statute actually exempts thousands of facilities. So what we are talking about here when you think of the classic Bhopal disaster of poison gas drifting out of a plant endangering people—and in this country we have hundreds of plants that can do that.

In looking at the tiering of DHS, if you separate that by risk issue, or I should say security issue, the release issue security facilities in Tiers 1 and 2 totals 35. That is totaling, in all 4 tiers, 370 facilities. That data is 2011 so it may be slightly less now. The point is that less than 10 percent of the facilities that you think of as the 3,900 CFATS facilities may be chemical disasters in the sense we all think of it as. And that is because they are being regulated by other programs like the MTSA, which look at more the water access of the facility.

Major facilities in the country, like this Keeney plant, probably the highest-risk facility in the United States, is regulated by MTSA. That facility puts 12 million people at risk. They, for 2 years on their Web site, say they are converting. We hope they are. Clorox converted all of their facilities in 3 years eliminating these risks to 13 million people. And we say risk, we mean a consequence; we mean the poison gas like chlorine that can drift 14

to 20 miles from a facility and put everyone downwind in danger of pulmonary edema, which would mean your lungs would literally melt. You would drown in your lung fluid. Those who would survive could have long-lasting, lifelong health problems.

So when we hear about the rush to approve security plans now, and were not comforted by the 7- to 9-year schedule GAO brings out, we are also not comforted by the fact that it is not a complete deck that we are dealing with here. So approval of a plan doesn't necessarily make it secure and it certainly doesn't make it no longer vulnerable. The CEO of DuPont admitted that if an airplane or a small helicopter coming into a plant couldn't be stopped by fence-line security, which is the entire basis of this kind of security.

Similar communities living near these plants are not comforted by these Alternative Security Plans developed by industry lobbies. They have heard too often when they have sheltered in place, or see explosions and flares and fires—were averaging about 45 a year, by the way, at refineries—that everything is oK. There are no dangerous levels of chemicals released.

So when you look at our testimony, look at the people who we have quoted in there, but also look at the Center for American Progress reports we sited, which identified hundreds of facilities that have converted and eliminated these risks to millions of people. We think any plant that can convert should be required to convert and, in fact, the CEP studies found that 87 percent of those converted that were surveyed did so for $1 million or less; 1/3 expected to save money. So this is good business. It also means eliminating liability and regulatory obligations.

And I have much more to say but I will wait for your questions. Thank you again for allowing us to appear today.

[The prepared statement of Mr. Hind follows:]

702 H Street, NW, Suite 300, Washington, DC 20001
Tel: 202-462-1177 □ Fax: 202-462-4507
1-800-326-0959 □ www.greenpeaceusa.org

Before the
Committee on Energy and Commerce
Subcommittee on Environment and the Economy
U.S. House of Representatives

The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update

Testimony of:
Rick Hind, Legislative Director
Greenpeace

Department of Homeland Security Regulations Leave Millions of People at Risk

Requirements for Safer Chemical Processes Will Eliminate the Catastrophic Consequences of an Attack, Accident or Natural Disaster

March 14, 2013

Introduction:

Mr. Chairman, thank you for the opportunity to testify today. My name is Rick Hind. I am the Legislative Director of Greenpeace and I have worked on this issue for more than a decade. I commend you for holding this hearing. I hope we can find ways to make sure our children do not inherit the catastrophic threats we face today.

Summary:

1) There are often many voices not at the table in Washington when important issues are discussed. In this case, it's the safety of more than 100 million Americans who live and work in "vulnerability zones." I prefaced my testimony with some wise words from a few them.
2) The catastrophic hazards we face are unimaginable and have not diminished but instead have grown.
3) The statute that authorizes the Department of Homeland Security's (DHS) Chemical Facilities Anti-Terrorism Standards (CFATS) was not designed to protect those who work in or live near high risk chemical facilities and it should be overhauled.
4) Cost-effective safer chemical processes are available for most high risk chemical processes and they should be required where ever feasible.
5) These hazards can be compounded by new threats such as cyber attacks while the old ones linger and even grow.

I look forward to answering your questions.

Preface: Some of The Voices You Should Invite to the Next Hearing:

"Should there be a successful terrorist attack on a chemical facility, the first question policy makers will be asked is this: 'Why, when you've known for more than ten years that America's chemical facilities were vulnerable to terrorist attack, did you consistently fail to take the steps needed to reduce that vulnerability and save lives?'
"Members of Congress need to think long and hard about how they'd answer that question if they continue to avoid taking the sensible steps required to make these facilities safer and less vulnerable to acts of terrorism."
-- Bob Bostock, Special Assistant to the Administrator (EPA) for Homeland Security (2001-2003)

"According to the 9/11 Commission, urgent warnings were ignored before the September 11th attacks. In addition, the Commission concluded that our government's first failure was a 'failure of imagination.' My husband was a victim of that failure.
"Yet today we continue to lack the imagination to prevent another tragedy. While we are all aware of the vulnerability and catastrophic hazards posed by our nation's highest risk chemical plants, we also know much more about the many safer chemical processes that can eliminate a plant's attractiveness as terrorist target.
"The fact that special interest lobby groups and allied politicians want to stand in the way of requirements to prevent such a disaster is unthinkable. I fear that when we suffer a catastrophic failure or attack at one of these facilities, those same elected officials will finally learn that the loss of human life is not worth the campaign dollars of moneyed special interests. Of course, by then, it will be too late."
-- Kristen Breitweiser, 9/11 widow

"In the event of a catastrophic chemical release in a major U.S. city, first responders would likely face the same fate as thousands of workers and community residents who would quickly be overcome by poison gas before they had a chance to evacuate. In addition, our emergency room capacity to treat thousands of poison gas victims on such a mass scale would be overwhelmed. Preventing such a disaster is the only effective means of treatment."
-- Peter Orris, MD, MPH Professor and Chief of Service, Occupational and Environmental Medicine University of Illinois Hospital and Health Science System

"Our members work in many of these facilities. We know how vulnerable they are, not just to terrorist attack, but to plain old accidents caused by any number of system failures."
-- Michael J. Wright, Director of Health, Safety and Environment United Steelworkers

"Early in my career as a Fire Fighter, I responded to an accident at a chemical plant. As the workers were evacuating, we were going into the plant, unsure of what dangers we would encounter and unsure of our own survival. The risks to both fire fighters and plant employees have increased as a result of more chemical plants in urban areas and the threat of terrorism. These risks can be reduced using safer alternatives and safer chemical processes that can prevent catastrophic events and save lives.
"New regulations are needed to require the use of safer and more secure alternatives where ever they are feasible to lower the risk to first responders, plant employees, and residents in the surrounding communities."
--Fire Captain Ed Schlegel, Ret. County of Los Angeles Fire Department

"There are 473 chemical plants in the U.S. that each put 100,000 or more Americans at risk of a Bhopal-like disaster. In addition, several thousand other plants also use and store poison gases such as chlorine and anhydrous ammonia on their property. Too many of these facilities are in lower-income neighborhoods and communities of color. The families in these communities have already waited too long for the federal government to make these neighborhoods safe from the dangers posed by these plants. "The government needs to stop pointing fingers and take responsibility to eliminate the risks these facilities pose and prevent an avoidable chemical disaster."
-- Stephen Lester, Science Director Center for Health, Environment & Justice Falls Church, VA

"How many lives must be lost before we have a policy that fully protects our communities and workers?"
-- Richard Moore of Los Jardines Institute (The Gardens Institute), and former chair of the EPA's National Environmental Justice Advisory Council

"Sheltering in place does not protect the health and well being of residents and communities. Requiring the use of safer alternatives will provide communities real protection from needless catastrophic hazards."
-- Michele Roberts, Environmental Justice Health Alliance

"Regrettably, our world is becoming more dangerous and risky, and policymakers can ill-afford to ignore the potential of risk prevention as another element of mainstream mandatory regulation. Clearly, the risk prevention paradigm raises significant design and implementation issues that require careful attention and reasonable resolution. Yet,

these issues are not unlike those faced by existing risk management programs and, thus, justify caution rather than rejection of this valuable regulatory approach."
– Timothy F. Malloy University of California, Los Angeles Law School

Conventional Security Will Not Protect Millions At Risk:

The September 11th terrorist attacks successfully used our own infrastructure against us with tragic results. They also demonstrated that tight perimeter security, such as at the case of the Pentagon, is incapable of preventing such attacks. Should a chemical plant be targeted, a truck bomb, a small plane, helicopter or a high powered rifle could render our current reliance on fence-line security useless.

The vulnerability of U.S. chemical plants to terrorism, natural disasters or serious accidents such as the 1984 disaster in Bhopal, India are now a given. The potential magnitude of these risks far surpasses the 9/11 attacks. Once a large release of a poison gas such as chlorine has occurred it can remain dangerous 14 miles down wind in an urban area (20 miles in a rural area) and immediately put the lives of thousands of people at risk. A November 2012 Congressional Research Service (CRS) analysis of Environmental Protection Agency (EPA) data identified 89 chemical facilities that each put 1,000,000 or more Americans at risk.

The nature of these risks meets any definition of a weapon of mass destruction. The manner in which people could be killed and injured is terrifying. Poison gases such as chlorine can literally melt the lungs of its victims causing them to drown in their own lung fluid (pulmonary edema). Survivors could be left with crippling life long disorders.

Following the 9/11 attacks it was reported that 9/11 ringleader, Mohamed Atta, visited a Tennessee chemical plant asking lots of questions (December 16, 2001 Washington

Post). In 2007 at least five successful terrorist attacks in Iraq used relatively small (150 pound) cylinders of chlorine gas to kill dozens of people. As a result the Department of Homeland Security (DHS) began briefing local bomb squads and chemical plants across the country. In April 2007 USA Today reported on the thefts of 150 pound cylinders of chlorine gas occurred in California prompting questions by members of Congress to the DHS about their response to these thefts.

U.S. chemical facilities were never designed to defend against terrorist attacks and predicting where the next attack will take place is a fool's errand. No one predicted that Timothy McVeigh would attack the Federal Building in Oklahoma City in 1995, killing 168 innocent people.

Industry leaders readily acknowledged this. In 2007 duPont Chairman Charles O. Holliday Jr. told the media that he worries most about a computer system failure or a security breach at one of the company's chemical plants around the world. "I feel very comfortable that we've taken all the reasonable steps, but obviously if someone wants to fly an airplane into a plant, it's very hard to guard against it," said Holliday.

Security experts such as Stephen Flynn, Senior Fellow in National Security Studies at the Council on Foreign Relations warned in his 2007 book, The Edge of Disaster:

> "...While attacks on the electric grid, oil and gas facilities, major ports, and the food-supply system have the potential to create the greatest cascading economic effects, it is chemical facilities near urban population centers that have the potential to inflict the greatest casualties...In most cases, chemical plants that threaten nearby populations can switch to less dangerous substances. This practice is known as 'inherently safer technology,' or IST...Without a strong mandate from the federal government, it's unrealistic to think they ever will. Yet voluntary compliance is the premise of the legislation Congress passed last fall [2006]; the new rules rest on the assumption that companies will now suddenly begin taking steps they have so far refused to contemplate."

A Successful Attack Would be Catastrophic:

--- In July, 2004, the Homeland Security Council estimated that an attack on a single chlorine facility could kill 17,500 people, severely injure an additional 10,000 and result in 100,000 hospitalizations and 70,000 evacuations.

--- In January, 2004, the U.S. Naval Research Laboratory testified before the Washington, D.C. City Council warning that 100,000 people could be killed or injured in the first 30 minutes of a catastrophic release of a tank car of chlorine or similar chemical within blocks of Capitol Hill. They further estimated that people could "die at rate of 100 per second."

--- In June, 2003 FBI specialist on weapons of mass destruction, Troy Morgan, in a speech at a chemical industry conference warned, "You've heard about sarin and other chemical weapons in the news. But it's far easier to attack a rail car full of toxic industrial chemicals than it is to compromise the security of a military base and obtain these materials."

Current DHS Rules (CFATS) are Fatally Flawed:

The best that can be said for the DHS's chemical security regulations known as "Chemical Facilities Anti-Terrorism Standards" (CFATS) is that they represent an official recognition of the widespread vulnerability of U.S. chemical plants to terrorism. Unfortunately the 744-word "rider" (Section 550) to the Homeland Security Appropriations Act 2007 was designed to authorize "interim" regulations that were expected to expire on October 4, 2009 but have since been given a series of short-term extensions.

The DHS rules finalized on November 20, 2007 fail to provide any authority to truly prevent chemical disasters whether triggered by terrorism, natural disasters or industrial accidents. As a result they leave one of our country's most vulnerable sectors of infrastructure inherently hazardous to millions of Americans living down wind of these facilities. That said, we applaud the hard work and dedication of DHS employees who have attempted to secure these facilities through conventional means with limited authority and huge gaps in the scope of the program. Without complaining about it they have inherited a fatally flawed statute which they endeavor to implement.

To the DHS's and EPA's credit they have repeatedly asked Congress for prevention authority. http://www.dhs.gov/ynews/testimony/testimony_1301517368947.shtm

In November of 2009 the House passed permanent, comprehensive legislation (H.R. 2868) that also included the DHS and EPA recommendations on prevention and eliminating security gaps but it never became law. If enacted H.R. 2868 would have seamlessly continued CFATS while addressing the major flaws in the underlying statute, giving the public confidence that they would be spared preventable disasters.

Specifically, the underlying statute (Section 550) which authorized CFATS:

- **Bars the DHS from requiring any "particular security measure," including safer chemical processes, what Senator Lieberman (I-CT) called, *"the only foolproof way to defeat a terrorist determined to strike a chemical facility."* It therefore fails to reduce the consequences of an attack at any of approximately 4,000 "high risk" chemical facilities now in the program:** H.R. 2868 conditionally required safer chemical processes. (Section 2111)
- **Exempts thousands of the 12,361 chemical facilities in the EPA's chemical disaster program, including an estimated 2,400 U.S. drinking water & waste treatment plants, and hundreds of chemical facilities located on navigable water ways including a majority of the U.S.'s 150 refineries:** H.R. 2868 covered all of these facilities. (Section 2103)
- **Fails to require deadlines for the completion of vulnerability assessment and facility security plans, or deadlines to notify facilities of a disapproval of security**

plans: H.R. 2868 set deadlines for completion of vulnerability assessments and security plans. (Section 2103)

- **Fails to authorize unannounced inspections or increased inspectors:** H.R. 2868 authorized unannounced inspections and added at least 100 new inspectors.(Section 2104)
- **Fails to require annual progress reports to Congress on the numbers of security plans approved & disapproved, numbers of compliance orders and penalties issued, etc:** H.R. 2868 required annual progress reports to Congress on security plans approved & disapproved, compliance orders, and penalties issued. (Section 2119)
- **Fails to provide for citizen enforcement suits or petitions of the government to ensure implementation of required programs, or protection for whistleblowers:** H.R. 2868 provided for citizen enforcement suits, petitions and whistleblower protections. (2116, 2117 & Sections 2108)
- **Fails to provide funding to convert publicly owned water treatment systems or private chemical facilities to safer chemical processes:** H.R. 2868 provided grants for the conversion to safer processes at publicly owned water treatment plants and privately owned facilities. (Section 1433). An in independent analysis of H.R. 2868 showed that 8,000 jobs would have been created, benefiting publicly owned water systems and the chemical industry sectors the most: http://www.misi-net.com/publications.html
- **Fails to require meaningful involvement of plant employees in developing security plans:** H.R. 2868 provided participation in the development of security plans. (Sections 2103 & 2115).

Complaints about the DHS CFATS program have centered around the slow pace of approving site security plans (SSPs) and the general lack of transparency of the DHS in too many aspects of the program. Again, H.R. 2868 would have put the DHS on a schedule and made them and the industry more accountable through unannounced inspections, reports to Congress, citizen enforcement suits and petitions, etc.

A faster pace in the CFATS program envisioned in H.R. 2868 would also have coincided with a faster pass in reducing hazards and the consequences of a successful attack. The rush to approve SSPs in today's CFATS program, however, does not necessarily build public confidence. When passengers face a flight delay of an airliner, they are frustrated but they also don't want the flight rushed onto the runway at the expense of safety.

The adoption of Alternative Security Plans (ASPs) developed by the chemical industry lobbying organizations is also not comforting to people living within vulnerability zones. They have too often "sheltered in place" or been assured that strange odors, flares, fires or even explosions "released no harmful levels" of dangerous substances (U.S. refineries have reported an average of 45 fires per year since 2008). We are unaware of any ASPs that require disaster prevention measures such as safer chemical processes.

Conspicuously absent from oversight hearings on CFATS are questions about prevention and why the DHS has not issued a 19th Risk Based Performance Standard to formally encourage high risk facilities to evaluate safer more secure chemical processes or "methods to reduce the consequences" of an attack. This idea was raised by Senator Lieberman (I-CT) in his formal comments on the CFATS rules in 2007.

Greenpeace has also asked the DHS, for more information on the facilities that have legitimately left the CFATS program because they no longer use or store chemicals of interest (COI). This is very good news but without giving away confidential business information, concrete examples would be more useful to other high risk facilities which may also want to reduce their liability, save on conventional security costs and have fewer regulatory obligations. It is not, however, useful to keep secret those facilities that are no longer in CFATS because they are no longer considered high risk.

Currently the DHS has only approximately 35 facilities in the two highest risk Tiers (1 and 2) that are considered "release" category facilities out of a total of about 579 facilities in those two risk tiers. This may be a symptom of how many high risk facilities are exempt from CFATS. Meanwhile in the EPA's RMP program there are 473 facilities

that each put 100,000 or more people at risk. If CFATS were a comprehensive program all of those facilities would be in risk Tiers 1 or 2.

Some of the highest risk facilities in the country are even more loosely regulated under other statutes such as the Maritime Transportation Security Act (MTSA), Clean Water Act and Safe Drinking Water Act. None of these statutes has any prevention requirement and the MTSA has also been the industry lobby's model for ASPs. Some of the highest risk chemical facilities in the country are exempt from CFATS because they are located on a navigable waterway and therefore regulated by the Coast Guard under MTSA.

We also have serious concerns about the Chemical Sector Critical Infrastructure Partnership Advisory Council (CIPAC) that operates autonomously and provides far too much access and opportunity for influence by the regulated industry over its regulator both in the development of rules and their implementation. For more details, see the November 25, 2010 Washington Post story on CIPAC:

http://www.washingtonpost.com/wp-dyn/content/article/2010/11/24/AR2010112407022.html

The only non-governmental members of the Chemical Sector CIPAC are chemical industry lobbying organizations or chemical companies. Although the DHS operates several committees under the Federal Advisory Committee Act (FACA), but the CIPAC is exempt from FACA regulations and most of its activity is done behind closed doors. Even the names of the individuals representing the trade associations are kept secret. The secrecy is rationalized as necessary to encourage candor by the industry. Rather than receiving "candid" comments from industry lobby groups who have led efforts to kill prevention policies, the DHS should seek out candid input from all stakeholders.

Currently no residents living near or rank and file employees working in high risk plants, including community organizations or unions, technical experts from academia or any nonprofit organizations that do not represent the industry are allowed to participate in CIPAC. The Washington Post reported on this in 2010:

http://www.washingtonpost.com/wp-dyn/content/article/2010/11/24/AR2010112407022.html

CIPAC's budget is more than $1 million a year and its charter expires March 16, 2014. Secretary Napolitano has authority to terminate the council at anytime or allow its charter to expire and create a FACA council that represents all stakeholders.

The CIPAC's influence is magnified by the DHS's limited authority and scope. One DHS staffer working on CFATS confessed to us a few years ago that they had never seen so much industry presence in other government agencies before and didn't feel comfortable with it. We have seen this first hand at annual public meetings of the Chemical Sector CIPAC. The DHS officials almost appear obsequious in their posture to the industry representatives. When prevention was discussed there were audible snickers in the audience.

The legislation (Section 550) which authorized CFATS was never intended to be a comprehensive statute. Senator Susan Collins (R-ME), chair of the Senate Homeland Security and Governmental Affairs Committee addressed this in her February 7, 2007 comments to the DHS:

> ***"In drafting Section 550, the intent of Congress was clear and unambiguous – this statutory provision provides the Department strong, interim authority for up to three years until permanent, comprehensive authority can be enacted...***
> ***"Section 550 was a streamline version of chemical security legislation; it was not the comprehensive authorizing legislation that Congress intended to be the final authority on this matter...***

"The Department does not have broad discretion to regulate beyond the interim three-year period without a comprehensive authorization from Congress. Any contrary interpretation of the 'sunset' provision is plainly wrong."

Since 2009 the Number of High Risk Chemical Plants Has Grown:

A November 16, 2012 CRS update of the number of high-risk chemical facilities in the EPA's chemical disaster or Risk Management Program (RMP) shows a growing number of chemical facilities that each put thousands of people at risk of a catastrophic chemical release. https://www.documentcloud.org/documents/557127-crs-rmp-update-11-16-12.html

In 2012, there were 12,440 EPA facilities nationwide that possessed thresholds quantities of ultra-hazardous chemicals requiring reports to the EPA of their "worst case" disaster scenarios. This was an increase of 79 facilities over the CRS's 2011 update on this EPA program. https://www.documentcloud.org/documents/557129-crs-update-of-us-rmps-state-by-state-4-12-11.html

The increase in 2012 included 28 additional facilities that put between 10,000 and 99,999 people at risk in the following states: Arizona, California, Colorado, Kansas, Louisiana, New Jersey, New Mexico, New York, Ohio, Oregon, Rhode Island, South Dakota, Texas, Utah, and Washington.

The 2011 CRS update also showed an increase of 332 in the total number of RMP facilities over the 2009 CRS update. https://www.documentcloud.org/documents/557128-crs-update-2009.html

Smart Security Eliminates the Catastrophic Consequences of an Attack:

In February 2008, the CEO of Association of American Railroads said, ***"It's time for the big chemical companies to do their part to help protect America. They should stop manufacturing dangerous chemicals when safer substitutes are available. And if they won't do it, Congress should do it for them...."***

The good news is that there are many commercially available safer processes for virtually all of the poison gas or toxic-by-inhalation (TIH) processes that pose the greatest risks to major urban centers. The Center for American Progress (CAP) has done several reports analyzing EPA's Risk Management Program data and in 2006 identified 284 facilities that have converted since 1999. See full report at:

http://www.americanprogress.org/issues/2006/04/b681085_ct2556757.html

Examples of conversions from TIH chemicals:

--- The **Blue Plains sewage treatment plant in Washington, D.C.** halted its use of chlorine and switched to a safer chemical process ninety days after the 9/11 attacks due to fears of another attack. The plant had seven 90 ton rail cars of chlorine on sight following the 9/11 attacks. The conversion cost approximately $0.50 per year for each water customer.

--- By mid-2012, the **Clorox Company converted all of its U.S. facilities** to "strengthen our operations and add another layer of security," according to their CEO Don Knauss. Clorox also indicated that these changes "won't affect the size of the company's work-force." This conversion eliminated Clorox's bulk use of chlorine gas and catastrophic risks to more than 13 million people in nearby communities.

http://investors.thecloroxcompany.com/releasedetail.cfm?ReleaseID=420583

The CAP analysis also showed that 87% of the converted facilities spent $1 million or

less and one third expected to save money, particularly from reduced liability costs and reduced regulation compliance costs. Clearly these conversion costs pale in comparison to the billions of dollars incurred in disaster response, relocating communities, defending against personal injury law suits or resolving environmental clean-up liability or long term conventional security costs which add nothing to the bottom line.

While the CAP analysis demonstrates the availability and feasibility of safer alternatives, most of the examples are not at the highest risk facilities. A 2008 CAP analysis identified 300 chemical facilities that together put 110 Million Americans at risk. At the current rate of voluntary conversions, without any new regulatory requirements, **it could take 40 years to eliminate these hazards to our major cities**.

The 2006 Government Accountability Office (GAO) report (GAO-06-150),"Homeland Security DHS Is Taking Steps to Enhance Security at Chemical Facilities, But Additional Authority Is Needed," concluded, "Implementing inherently safer technologies potentially could lessen the consequences of a terrorist attack by reducing the chemical risks present at facilities, thereby making facilities less attractive targets."

An earlier GAO report (GAO-05-165) identified chlorine gas and 90-ton chlorine rail cars as "among the top five terrorist-related wastewater system vulnerabilities." Among the top three recommendations: "Replacing gaseous chemicals used in wastewater treatment with less hazardous alternatives." In addition, the largest majority of experts gave replacing these chlorine facilities the highest priority for federal funding.

"The most desirable solution to preventing chemical releases is to reduce or eliminate the hazard where possible, not to control it. This can be achieved by modifying

processes where possible to minimize the amount of hazardous material used, lower the temperatures and pressures required, replace a hazardous substance with a less hazardous substitute, or minimize the complexity of a chemical process." -- **National Academy of Sciences** 2006

"As hard as it is to believe, the chemical industry has refused to take adequate precautions to safeguard its facilities and surrounding communities. Some plants have strengthened on-site security by adding guards, building fences or installing surveillance cameras. Others have committed to reducing or phasing out their use of highly hazardous processes or chemicals in favor of safer ones. Unfortunately, however, it is still business as usual at most plants. They continue to deal with high volumes of dangerous chemicals -- even when safer materials or processes are readily available. That is why the government must require industry cooperation in homeland security."
--- **Former Senator Gary Hart (D-CO)** ***Washington Post*** Op-Ed August 11, 2003

The Benefits of Safer Chemical Processes:

Risk Management Solutions estimated that a "chlorine spill scenario results in 42,600 total casualties, over 10,000 of which are fatal. Insurance claims covering these casualties would exceed $7 billion." **http://www.rms.com/NewsPress/PR_042904_CasualtyStudy.asp**

The use of safer chemical processes offer a more competitive and stable business plan with fewer regulations, potentially zero liability, sustainable profitability, better relationships with workers and neighboring communities and no threat of a catastrophic attack or accident. Specifically, the use of safer processes will likely result in a facility no longer being subject to DHS's CFATS or EPA's RMP regulations.

Obviously, chemical facilities located on site at nuclear power plants, drinking water treatment facilities, iconic facilities such as Disney World, etc. also need protection through conventional security means. Using safer chemical processes at these facilities, however, will also reduce the consequences of an attack on them.

Given DHS's finite resources and the late start the nation has in addressing chemical security it is urgent that we use safer processes to mitigate the consequence of an attack. By doing so we eliminate risks, safeguard communities and save scarce money and conventional security resources to protect facilities that cannot be neutralized as attractive targets (airports, U.S. Capitol, etc.).

A Comprehensive Program of Prevention Is Needed:

To truly protect employees and surrounding communities, our economy and national security a comprehensive program should include:
1) Requirements for the use of "smart security" to prevent the catastrophic consequences of an attack by implementing cost-effective safer and more secure chemicals and processes at all of the highest risk facilities.
2) Include all categories of facilities such as port facilities and water treatment plants.
3) Involve plant employees in developing plant security programs, including participation in workplace inspections, and provide employees with both an appeals and a waiver procedure to protect against excessive background checks.
4) Allow citizen suits and petitions to enforce the law and require reporting measures that strengthen accountability.
5) Allow states to set more protective security standards.
6) Require collaboration between the DHS, EPA and other agencies.

The Threats Continue to Linger and Unfold

Secretary of Defense Leon Panetta issued a warning to business executives in NY City regarding the increasing threat of cyber attacks last October. He said, "The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life..." He also gave the example of "computer

control systems that operate chemical, electricity and water plants and those that guide transportation throughout this country."

http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136

A November 21, 2011 MSNBC story reported, "Hacker says he penetrated the network of a South Houston, Texas, water-treatment plant to expose the inherent vulnerabilities in critical industrial control facilities and prove how easily they can be compromised." The potential consequences of a real attack could result in the release of the contents of a 90 ton chlorine rail car which are routinely used to store chlorine gas at water treatment plants. http://www.msnbc.msn.com/id/45394132/ns/technology_and_science-security/#.TsvL17LNIGUA

A November 2010 Washington Post report revealed that the Lashkar-e-Taiba terrorist organization that committed the 2008 attacks in Mumbai, India, had also asked a now convicted U.S. ally to "conduct surveillance of an unnamed chemical plant in Maryland." Lashkar-e-Taiba was reportedly gathering intelligence on U.S. targets as early as 2001. http://tpmlivewire.talkingpointsmemo.com/2010/11/the-man-behind-mumbai.php

On August 2, 2010, two men were convicted of plotting to blow up jet-fuel tanks at John F. Kennedy International Airport, a plan authorities said was meant to outdo the September 11, 2001 attacks. http://www.washingtontimes.com/news/2010/aug/2/ny-jury-convicts-2-jfk-airport-tank-blast-plot/?page=1

Since before 9/11, the Kuehne Chemical Company in South Kearny, NJ has put up to 12 million people at risk of a chemical disaster due to their chlorine gas storage adjacent to

New York City. Former counter terrorism operative for the CIA, Charles Faddis visited the Kuehne plant in July 2009. In his book Willful Neglect he wrote:

> ***"Anybody with minimal training in breaching and some basic equipment can go through those gates in moments. After that, it is all over. There is no way on earth that any guards inside are going to react, repel a team of armed assailants and prevent the inevitable. Every tank in the facility is going to be ruptured, either by satchel charges or vehicle borne explosive devices, and what happens in the surrounding area is then going to be purely a function of meteorological conditions."***

(For approximately two years Kuehne's web site has stated that they were in the process of converting to a safer process but no details have been made public.)

On August 29, 2007, a single railroad tank car of chlorine somehow rolled out of a rail yard in Las Vegas, Nevada and ran for twenty miles before it was secured. During that twenty mile run it rolled through the heart of Las Vegas and densely populated neighborhoods. Even though the car reached speeds of up to fifty miles an hour, it miraculously didn't derail or release the chlorine. http://www.lvrj.com/news/9466232.html

"You know, the threat is just staring us in the face. I mean, all you'd have to do is to have a major chemical facility in a major metropolitan area go up and there'd be hell to pay politically," says Rudman. "People will say, 'Well, didn't we know that this existed?' Of course, we knew." --- **Former Senator Warren Rudman (R-NH)** ***CBS 60 Minutes***

Mr. SHIMKUS. Thank you, Mr. Hind.

Now, I would like to recognize myself for the first 5 minutes of questions.

I want to start off whatever script I was given to ask Mr. Scott a question. Were you in the room when Representative McKinley was asking about the risk assessment issue? And, of course, DHS responded that, well, we don't know of any identifiable risks. And I am paraphrasing here—then the question went to about European security and DHS responded, well, we think we are the gold standard. Since you operate around the globe, does individual European countries or the EU at large have a CFATS-type program?

Mr. SCOTT. No, but they are discussing a similar program. The difference you have there, you are working between various countries. But they do have regulations in place like the Seveso regulations that impact offsite types of emergencies. The EU is having a conversation about are there any general rules and regulations that we can put in place? They have been talking. They have talked with DHS in the past. We are working with——

Mr. SHIMKUS. Maybe they should talk with our GAO, our Government Accounting Office, then DHS.

Mr. SCOTT. Yes. Well, DHS is a standard; I wouldn't say it is a gold standard. But the folks overseas are looking at similar directions to go, both in transportation and site security. But we also have a lot of work that we have done over there through the Responsible Care Code. It is a global code. So that has been implemented. And a lot of the same safety and security cultures that are in place in the U.S. are in place throughout Europe.

Mr. SHIMKUS. I appreciate that.

Now, for Mr. Allmond and Mr. Scott and Mr. Drevna, GAO reports—and you all have heard these conversations earlier today—that DHS largely disregards vulnerability, economic criticality, and threat assessments as part of the risk calculations making CFATS a modified consequence prevention-only program. Are you concerned your members might be overregulated or under-tiered? Mr. Allmond?

Mr. ALLMOND. Well, certainly these revelations are concerning. And it is going to take me some time to get back to my members to find out from their perspective how they would like to proceed. I think completely stopping the CFATS program from going forward probably would be overboard. Perhaps some components could go forward. But certainly——

Mr. SHIMKUS. OK. But you were here during the testimony. Do you think that some of your folks are overregulated or under-tiered? It is pretty easy——

Mr. ALLMOND. Well, at this point it seems like that may be the case.

Mr. SHIMKUS. Thank you. Mr. Scott?

Mr. SCOTT. I would say yes. Looking at the variability in the sites that we have that are covered, there is a lot of question on how we got where we got.

Mr. SHIMKUS. Mr. Drevna?

Mr. DREVNA. I concur.

Mr. SHIMKUS. You have heard from panels one and two that DHS has collected a lot of information that it will not use in risk assessment. Are you comfortable with that? Mr. Allmond?

Mr. ALLMOND. No, we are not.

Mr. SHIMKUS. And why?

Mr. ALLMOND. DHS should use the information that is given to them. As has been testify before, there has been an enormous amount of resources given to—from our side—given to the Department that we are compelled to do and there is an understanding that the Department is going to use that information.

Mr. SHIMKUS. Mr. Scott?

Mr. SCOTT. I agree. The inefficiency in the process caused a lot of unnecessary work, a lot of information that they have never used, and we don't know where the information went. It seems like they felt like they had the answer before we started the process.

Mr. SHIMKUS. Mr. Drevna?

Mr. DREVNA. Yes. And I would like to add to that, Chairman Shimkus, that in chemical facilities you are changing processes constantly. So we are submitting information, it goes somewhere, lots of information, up to 900 questions on some things. It goes somewhere. Whether it is used or not, probably not all of it. Again, if it is vital, perfect. If it is not, let us work with you to get it done. But then you change your process again, you may have to go through the whole thing again because these things are not static kinds of plants. We are always changing volumes and chemicals.

Mr. SHIMKUS. Mr. Scott?

Mr. SCOTT. I would like to add to that. That is one of the big issues that we have is we typically have larger plants, a lot of processes in those plants and we are required to submit any time we change anything in the process, make another submission. That puts you back to square one in the whole process.

Mr. SHIMKUS. And just because my time is getting short, and Mr. McNerney is not here, but he talked a lot about cyber stuff. So you have got all this data going somewhere. If it is not being used, why it is being held and what is the risk of that being pulled out to make your facilities less secure. Is that a risk? Mr. Scott?

Mr. SCOTT. Well, it is a risk whenever you release the information that you hope it is going to be secure. But in the earlier panel, we also heard that, well, maybe we can declassify that so everybody can talk about it. And I am concerned about the level of declassification. If it is just open to the public, that is a real security concern.

Mr. SHIMKUS. Anyone else while my time is expired? Mr. Drevna?

Mr. DREVNA. I would like to add to that. You are probably one hit of forward or reply all from exactly what Mr. Scott was just talking about.

Mr. ALLMOND. Absolutely.

Mr. SHIMKUS. Mr. Allmond. OK. Thank you. The chair now recognizes ranking member, Mr. Tonko, for 5 minutes.

Mr. TONKO. Thank you, Mr. Chairman.

And to the gentleman on the panel, thank you for your time and your input today.

To the industry witnesses, did you participate in GAO's survey?

Mr. ALLMOND. Oh, SOCMA did, yes.

Mr. SCOTT. ACC did, yes.

Mr. DREVNA. Yes, sir.

Mr. TONKO. So you all did.

GAO found that transparency in the tiering process should be improved. Can each of you state whether you agree with this GAO conclusion?

Mr. ALLMOND. I will say absolutely. As Mr. Scott was saying, a lot of times these facilities give information without getting a really detailed understanding about why they got the tier level they did.

Mr. SCOTT. All of the information was submitted. I absolutely think it should be more transparent with the people that we were supposed to be working as partners.

Mr. DREVNA. I agree, Mr. Tonko. But I will say that the process has somewhat improved. We have got a long way to go, but we weren't where we were before this report came out.

Mr. TONKO. Mr. Drevna, you talked about the PSP process——

Mr. DREVNA. Yes, sir.

Mr. TONKO [continuing]. And utilizing it more readily.

Mr. DREVNA. Yes, sir.

Mr. TONKO. Can you just develop that a bit for me?

Mr. DREVNA. Well, at refineries and petrochemical facilities, you have constantly—you have your own employees—but you have constant, contractors coming in and out, turnarounds, changeovers, et cetera, and they are authorized, the contractors, under TWIC, Transportation Worker Identification Credential. And what the DHS will tell us is that, well, we are coming up with a remedy for that but those rules aren't going to be ready for who knows how many more years. Meanwhile, we have to, perhaps, have other identification notices or identification cards for the various employees and contractors.

It is sort of like if I can make some sort of an analogy, sort of like me or you going through an airport and you have to have your passport to go through the first gate, and your driver's license you through the second, and maybe your voter ID card to go through the third or whatever. But it doesn't make any sense. So you talk to us in industry and we usually object to the one-size-fits-all approach and maybe that is not applicable. But we need something that is not duplicative, time-consuming, and sometimes conflicting.

Mr. TONKO. Thank you. Thank you, Mr. Drevna.

Mr. Hind, you made mention, or I think to use your words, we are not dealing with a complete deck. Can you elaborate on that? What else should be done to make certain that we are providing for the public safety elements out there or in keeping with the mission of the legislation?

Mr. HIND. Well, if you look at the EPA's database through its risk management program, which is really kind of an imperfect larger universe of the facilities we are worried about, those that have off-site consequences, the total number of facilities in that program is 12,440 according to CRS' latest update in November. Of those, 2,500 plants each put 10,000 people or more at risk. Of the 2,500, some of them could put over a million at risk. In fact, 473 put 100,000 at risk. And so my question to the panel here is, which of your member companies are actually part of MTSA and exempt

from CFATS or part of a DOE program or even Defense Department? And I think that the numbers would be rather revealing in terms of which they are.

We have heard that Dow's largest plant the country at Freeport, Texas, is that MTSA facility. So that means there are huge holes, or as Congressman Waxman called them, gaps in the security and in terms of the continuity of security by the government accountability over the industry.

Mr. TONKO. Thank you. And from the public interest perspective, what are the problems with incorrect tiering of facilities?

Mr. HIND. You mean in terms of the way that the risk assessment has been conducted and so forth? Well, in our view, we are a little bit nervous to hear about economic considerations being added and also vulnerability. I think that all of these facilities are vulnerable. If somebody takes a small plane or hijacked it, all of the guards and cameras and gates are not going to be enough to stop a small plane, as the CEO of DuPont admitted years ago. So I think that, as the former EPA administrator Ruckels has warned, risk assessment is like a captured spy. If you torture it enough, you can get to say anything. And I fear that we are going down a slippery slope here, and what needs to be done is adding alternative assessment to the process. Each company should be going out and saying to the DHS, we have looked at all the alternatives and there is nothing feasible for facility, or we are like Clorox and we can convert. And then you have zero risk.

Mr. TONKO. Thank you. I think some of you might have a comment to that, too, or——

Mr. SCOTT. Yes, I just——

Mr. SHIMKUS. Without objection, we will continue for a minute to get a response. Mr. Scott?

Mr. SCOTT. OK. Yes, I would just like to reply on the MTSA question. There are several sites that are covered by MTSA, but rightly so. They have waterside security included on their security. But the Texas operation site is the one that Mr. Hind mentioned, which is our largest site. It is the largest chemical site in the United States. It is covered by MTSA so it does have different requirements. It also has exactly the same security upgrades already in place that are required of a Tier 1 CFATS site. So if you come down to Freeport operations or Texas operations, you will see we would be in full compliance with CFATS right now as a Tier 1 site. All of our MTSA sites are upgraded security-wise exactly the same as our CFATS sites. And all of our sites globally are tiered the same way and have security upgrades in place the same way. So I think that addresses the issue that we can have integration of the two systems very well.

Mr. SHIMKUS. Thank you very much.

The chair now recognizes the gentleman from Pennsylvania, Mr. Pitts, for 5 minutes.

Mr. PITTS. Mr. Drevna, did you want to add to that?

Mr. DREVNA. Well, if you don't mind, Mr. Chairman, thank you.

I agree with everything that Mr. Scott had said exponentially. But since the question was asked from the panel to the panel, in short of installing Patriot missile batteries at all facilities, I don't

see how we are going to stop anything from coming in from outside the gate like an airplane or helicopter.

Mr. PITTS. Mr. Allmond, you testified that DHS should be more willing to extend the amount of time a small or medium-sized facility has to respond to a post-inspection report. How much time is reasonable so that the small and medium-sized facility still feels the urge to promptly respond while also giving them the chance to provide a quality response?

Mr. ALLMOND. Yes. Thank you for that question. I think a minimum of 90 days will be sufficient.

Mr. PITTS. Do you believe DHS still has time to make program adjustments and will consider your perspective, and if so, what gives you that confidence?

Mr. ALLMOND. I do. In fact, I have already broached this concern with the Department and they have been receptive to hearing our proposal.

Mr. PITTS. Thank you. Mr. Drevna, your testimony discusses the importance your members place on getting a workable Personnel Surety Program. Is DHS addressing your particular concerns?

Mr. DREVNA. Well, we have been working with them, and as I said previously, ever since, the report came out and we have sat down—and I have to admit, there has been more transparency and they are willing to work with us. But we have got to establish the fact that we—you know, as I said before, the TWIC reader card implementation is years away. But we are in the process of doing all this now. So there has to be some meeting of the minds here that says, oK, let's get this done in a timely fashion so we can move on.

Mr. PITTS. Has AFPM tried to get an Alternative Security Plan approved by DHS for its members? What has been your experience with DHS in trying to advance——

Mr. DREVNA. Well, we support the alternative plans. We haven't particularly as an association done it, but our members have. And that is one of the things we keep, the tiering process, the kind of data that is needed. It is a little bit confusing between what is needed for the full assessment, what is needed to get you into a quicker AV alternative plan. So we are working with them. We support it and again, we are seeing the light at the end of this tunnel but we still have a ways to go.

Mr. PITTS. Assuming DHS, with the help from a Peer Review Panel, comes up with a better risk assessment model, when should it be applied to CFATS activities? Does it affect the speed with which your members would have their Site Security Plans reviewed and approved?

Mr. DREVNA. Is that for me, sir?

Mr. PITTS. Yes.

Mr. DREVNA. I believe it would. I mean, we have three members companies on that tiering panel. And we are confident that we are getting joint cooperation. Anytime you get three companies on the panel, a government panel, we are happy with that. But the proof is going to be at the end of the day with what is accepted and what isn't.

Mr. PITTS. All right. Mr. Scott, your testimony raised concerns about transparency by DHS officials because they did a poor job of communicating threat information to CFATS-regulated facilities.

Do you think DHS can formulate credible threat information and assessments?

Mr. SCOTT. I think they can give us the information that they have available to us. There is a NIAC study out that is on communications amongst the intelligence communities in the D.C. area and DHS did not come out very highly on that panel.

Mr. PITTS. Does it surprise you that GAO found that DHS really doesn't assess threat for 90 percent of terror threats at facilities with chemicals?

Mr. SCOTT. Threat typically is not discussed, and when you have a meeting with DHS, typically, it starts with there are no credible threats to the chemical industry at this time. We go on the premise that because we are part of the critical infrastructure, we are a potential threat or there is always a potential threat. That is the discussions we have always had.

Mr. PITTS. What recommendations do you have for DHS to improve its threat characterizations and communications?

Mr. SCOTT. You have to identify the baseline on the threats that you are going to address, and then you have to have plans in place to escalate your security programs accordingly as the risk increases.

Mr. PITTS. Do you agree with GAO that DHS assessment tools, particularly threat consequence and vulnerability ones, should be verified and valid before being deployed?

Mr. SCOTT. Yes, I do. Validity is important, yes.

Mr. PITTS. My time has expired. Thank you.

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

The chair now recognizes the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman. And obviously, our threat assessments are a work in progress because I remember in late 2001 there was in one of the caves in Afghanistan there was information on an attack on a refinery in Pasadena, California. It didn't take too long to know there are no refineries in Pasadena, California. But I represent Pasadena, Texas, and we have no shortage of refineries. And that was right after 9/11. Obviously, it was infancy.

And today, though, there is a lot—and I know at least in the industries that I work with in my area in East Harris County, the coordination between the federal agencies and our local police agencies is amazing. Now, I don't know what DHS does with the local law enforcement, the FBI, the Customs and Border Protection, the Coast Guard. In fact, I was at the Coast Guard facility in our district that now is co-located at a Coast Guard facility with the Harris County Sheriff's office boats, along with the Houston Police Department boats at the same location in our district in Galena Park, Texas. So, I mean, it is a work in progress.

Were you all here for the first panel? Do you feel confident that we are going to end up not having to jump through second hoops on your non-MTSA facilities and that the TWIC card is going to be able to be used? If you have a site that Dow does, for example, in Freeport, that the TWIC card works and you have a land-based site, the TWIC card will also, ultimately when they get through,

will also be able to be used for an ID at that land-based facility for Dow?

Mr. SCOTT. That is the direction that they are moving in. So yes, a TWIC card would be acceptable and usable at any of those sites. Yes.

Mr. GREEN. Well, Mr. Chairman, we need to just monitor that because I know we in the Subcommittee had that discussion for a number of years, and frankly, we probably wouldn't have gotten where we are without a great GAO study to show that the problem is within DHS.

For Mr. Drevna and Mr. Scott, over the past year, have you seen changes in outreach and cooperation from DHS and the industry, particularly as they relates to chemical and fuel and petrochemical manufacturers in the last year?

Mr. DREVNA. Yes. In the last year they have significantly improved the communications from DHS to their people in the field and from the people in the field to the sites. Yes.

Mr. GREEN. Well, and I understand in your testimony you are concerned that the transparency on the decision-making ought to be much better and our committee ought to be encouraging that. Now, I do have some concern about the information provided on your plant facilities, because again, the experience we have over the last 12 years is that if a lot of your information is given to DHS, it is public record. There are folks in part of the world who can, with the punch of a button, look up plant design and plant vulnerability. That should not be public record. And I am concerned about that.

We want transparency in the approval process but as much as I want as much public information for my constituents that live around and work on those plants, I also know I don't want to give a guide to somebody who wants to fly that Piper Cub over it. Is that some of your concern?

Mr. DREVNA. Absolutely. Like I said before, Congressman Green, we submit information and we submit it in good faith and——

Mr. GREEN. Well, you are required to.

Mr. DREVNA. But like I say, it is either one reply all or one forward button away from getting into the wrong hands.

Mr. GREEN. Well, I think in follow-up hearings we might have DHS come talk about what they do with information that is provided so it is protected. But I have to admit, Charlie, it is interesting, the ultimate 2nd Amendment is somebody having a Stinger missile to protect their plant or their house from a Piper Cub flying over it. I don't think we are going to get to that point. But I see planes fly over my plants literally every day when I am at home. And there is a special protection, though, you have to have special access to be able to fly over those facilities and no system is foolproof. But also, I don't know if I really want us to have to train our plant personnel to have a Stinger missile on their shoulder.

Mr. DREVNA. I would concur, Congressman Green.

Mr. GREEN. But Mr. Chairman, I appreciate the hearing. It seems like we made progress, but obviously DHS needs to come a little more with plants who, as I have said before, have made a million dollars in federal tax dollars, millions of dollars of investments and partnerships with our local communities that we still don't

know what hoops and what will be approved, whether it be Tier 1, 2, 3, or 4. And I would like to have some certainty there, and I know Greenpeace would like that to, and so would my constituents. Thank you.

Mr. SHIMKUS. The gentleman yields back his time.

We want to thank the third panel for being here and ask unanimous consent for 5 days for subcommittee members to submit opening statements for the record. Without objection, so ordered. We would also ask unanimous consent for 10 days to submit written questions for submittal to witnesses for an inclusion in the records. That also pertains to you all.

And inclusion of a letter, I ask unanimous consent for the inclusion of a letter from the National Association of Chemical Distributors to myself and Mr. Tonko—your staff has approved—dated March 12, 2013, on the CFATS program. Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. SHIMKUS. And the hearing is now adjourned.

[Whereupon, at 12:43 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. HENRY A. WAXMAN

I thank the Chairman for calling this hearing on this very important program. The Chemical Facilities Anti-Terrorism Standards Program, or CFATS, is a critical national security program designed to protect communities from potential terrorist attacks on industrial facilities with significant stores of dangerous chemicals.

Since 2001, federal officials, the Government Accountability Office (GAO), and outside experts have warned that the nation's drinking water utilities and chemical facilities remain vulnerable to terrorist attack.

Unfortunately, the CFATS program is a grave disappointment. At the end of 2011, we learned the program was in disarray. No facilities had approved site security plans. Homeland Security officials felt their enforcement authority was insufficient and ineffective. There were no procedures in place to document important programmatic decisions. No one on staff was even qualified to conduct a compliance inspection.

There has been some progress. We will hear from the Department today about their efforts to strengthen the CFATS program and the advances the Department has made since undertaking a serious internal examination of the program in 2011.

But today we will also hear from the Government Accountability Office, which has undertaken the first rigorous external accounting of the program. GAO has found that fundamental problems still plague the program. More work is needed before Congress and the American public can have confidence in the risk assessments that determine the potential dangers facilities pose.

Perhaps we shouldn't be surprised. CFATS was created in the sloppiest legislative fashion possible. It was established in 2006 by a provision tucked into an appropriations bill without the benefit of hearings or markups by the Committee.

The problems with the program are not all Congress' fault. Both the current and previous administrations have failed to implement the program effectively. The Department issued an interim final rule within six months of the law's passage. This rule determined what chemicals might be targets, how risk would be assessed, and what security standards would be applied. Given the quick action and limited statutory guidance, the rule was flawed. But now—six years later—it still hasn't been updated and improved.

In the 111th Congress, we worked on a bipartisan basis with industry, labor, and other affected stakeholders to methodically resolve each of the issues surrounding the CFATS program.

The result was H.R. 2868, the Chemical and Water Security Act of 2009, which passed the House by a vote of 230-193. That legislation would have addressed many of the challenges the program now faces, increased transparency and accountability, clarified the process for approving or disapproving site security plans, and set enforceable deadlines. It also would have strengthened security at covered facilities by

requiring assessment, and in particular circumstances, adoption of safer chemicals, processes, or technologies to reduce the consequences of a terrorist attack.

Unfortunately, that bill did not become law, and that opportunity to set this program on a more successful path was missed.

In the years since, this Committee has failed to develop comprehensive legislation to reform the CFATS program. It has also failed to offer any legislation to close security gaps or address security at water facilities.

This Committee needs to do more. Comprehensive legislation is long overdue.

I look forward to the testimony of the witnesses today, and I invite all of them and other stakeholders to engage with this Committee and help us seek solutions to a troubled, yet critically important anti-terrorism program.

Advancing **Stewardship**, Creating **Connections**

March 12, 2013

The Honorable John Shimkus
Chairman, Subcommittee on Environment and Economy
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Paul Tonko
Ranking Member, Subcommittee on Environment and Economy
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman and Ranking Member,

The National Association of Chemical Distributors appreciates the opportunity to comment on the Chemical Facility Anti-Terrorism Standards program. As the trade association representing our nation's chemical distribution industry, NACD offers a unique and important perspective on CFATS. NACD members process, formulate, blend, re-package, warehouse, transport, and market chemical products exclusively for an industrial customer base of more than 750,000. NACD members operate in every state in the continental U.S. and throughout all of North America through more than 1,500 facilities. Most NACD members are small businesses. The typical member is privately owned with $26 million in annual sales, 3 facilities, and 28 employees. More than 40 percent of NACD members are family-owned.

NACD members demonstrate our commitment to product stewardship through compliance with Responsible Distribution, our mandatory and third-party verified environmental, health, safety, and security program. NACD members have always focused on the safety and security of our workplaces and products. In response to the terrorist attacks of September 11, 2001, NACD became the first chemical trade association to mandate specific security measures for our members, and we continue to assess Responsible Distribution's security measures against current threats. Specific measures addressing security include:

- Developing programs that address security of a member's facility and the transportation of chemicals, including conducting a security vulnerability assessment
- Scrutinizing for-hire motor carriers for the security of chemicals in transportation
- Qualifying customers purchasing chemicals as prescribed by government regulations
- Verifying implementation of security measures by an independent third-party verification firm

1555 Wilson Blvd., Suite 700 Arlington, VA 22209 P: 703.527.6223 F: 703.527.7747 nacd.com

NACD members are more committed than ever to security. Last month, the NACD Board of Directors unanimously voted to create a specific Responsible Distribution Security Code to formalize and further emphasize these security measures.

Despite its slow start and programmatic challenges, CFATS is an important program that has spurred industry to develop consistently reliable approaches to chemical facility security, reducing our vulnerability to the threat of terrorist activity. As envisioned by Congress during its passage, CFATS provides an opportunity over time to improve public confidence that our nation's chemical facilities are secure not only from intentional releases, but against contamination and theft designed to create chemical weapons.

There has been much frustration, on Capitol Hill, in industry and even within DHS, that this program has been slow to develop. Moreover, since the November 2011 memo leak, it has been clear that the problems with the program have been severe and fundamental. While evident challenges remain, since that time, DHS has designed 95 actions plans to address the specific issues identified and has made at least some progress on each one, and completed many. As DHS is making progress on addressing these challenges and implementing CFATS, the importance of maintaining a well-funded program is greater than ever.

While improvements can and should be made in CFATS program, our industry is committed to working as a partner with both Congress and DHS to further the primary purpose of the program. We appreciate this Committee's vigilance and ask that you continue to support the program as the agency continues its efforts to make progress toward this critical program's basic mission of providing security and confidence in our nation's chemical management system.

Respectfully,

Chris Jahn
President

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

April 4, 2013

The Honorable Rand Beers
Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Under Secretary Beers:

Thank you for appearing before the Subcommittee on Energy and Power on Thursday, March 14, 2013, to testify at the hearing entitled "The Chemical Facility Anti-Terrorism Standards Program – A Progress Update."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Thursday, April 18, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Nick.Abraham@mail.house.gov and mailed to Nick Abraham, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

John Shimkus
Chairman
Subcommittee on Environment and the Economy

cc: The Honorable Paul Tonko, Ranking Member,
Subcommittee on Environment and the Economy

Attachment

Question#:	1
Topic:	ISCD's risk assessment approach 1
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: According to DHS's National Infrastructure Protection Plan (NIPP), risk is a function of three components—consequence, threat, and vulnerability—and a risk assessment approach must assess each. What's the effect of not considering threat or vulnerability for approximately 90% of regulated facilities?

Response: The current CFATS process considers all three components of risk—consequence, vulnerability, and threat—at various junctures throughout the process. The tiering process is primarily consequence driven, but threat and vulnerability are also considered in other parts of the CFATS process. However DHS is currently working to identify ways to further improve its tiering methodology, including how threat is applied to facilities possessing theft-and-diversion chemicals of interest and how vulnerability is considered throughout the risk model.

Question#:	2
Topic:	ISCD's risk assessment approach 2
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: Aren't you engaging an expert panel review?

Response: Yes, the Department has engaged an external peer review panel.

Question: What is the charge for this panel?

Response: The Department has asked the panel to review the CFATS risk tiering methodology and to comment on its strengths, weaknesses, and suitability to purpose.

Question: What is the timeline for them to report?

Response: The Department expects to receive the final report in September 2013.

Question: Do you plan to fully implement their recommendations?

Response: I expect the peer review to provide ideas on how DHS can enhance its tiering methodology models. After the Department receives the report, the recommendations will be reviewed and a determination will be made regarding the appropriateness and feasibility of implementing any recommendations.

Question: Will you apply it to your tiering process or some other part of CFATS?

Response: The peer review panel has been asked to provide recommendations on the tiering methodology, but may also provide supplemental thoughts on the CFATS process. ISCD will develop an integrated plan with timeframes and milestones that will set the terms for incorporating recommendations into an improved risk methodology, as appropriate.

Question: Will you apply it retroactively or prospectively?

Response: Without knowing the panel's recommendations, it cannot be determined at this time whether the peer review recommendations will be applied retroactively or prospectively.

Question#:	2
Topic:	ISCD's risk assessment approach 2
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: Given that past evaluations did not disclose problems with the current model, will the ongoing expert panel be in a better position to identify potential problems? Why?

Response: Previous evaluations identified some problems with the tiering methodology, and I believe the current peer review panel is in a good position to identify any remaining potential problems. As a part of the ISCD Action Plan implementation, ISCD committed to conduct a thorough review of the risk assessment process. ISCD has implemented a phased approach which includes: documenting all processes and procedures relating to the risk assessment methodology; conducting an internal NPPD review of the risk assessment process; and initiating an external peer review of the risk assessment methodology. ISCD has completed the first two phases and has provided this documentation to the peer review panel. The panel is comprised of eight members with expertise in risk analysis, infrastructure security, toxicology, chemical process safety, chemical intelligence.

Question#:	3
Topic:	ISCD's risk assessment approach 3
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: If the tiering approach is found to be faulty or requires adjustments as a result of the expert panel review, will this change the current list of tiered facilities? Will currently regulated facilities have to go through the process again?

Response: Without knowing the peer review panel's recommendations, the Department cannot say how the recommendations will impact the current list of tiered facilities. However, when the Department receives the recommendations, both Congress and industry stakeholders will be informed of any possible impact to the list of tiered facilities.

Question: To what extent does the current list of regulated facilities accurately reflect the chemical facility terrorist threat in the United States?

Response: The Department believes that high-risk chemical facilities continue to present an attractive target for terrorists. Many of these potential targets are regulated under the CFATS program; however, a number of chemical facilities are exempt from CFATS by statute including those regulated under the Maritime Transportation Security Act (MTSA), Public Water Systems, as defined in the Safe Drinking Water Act, Water Treatment Facilities, as defined in the Federal Water Pollution Control Act, facilities owned or operated by the Department of Defense or the Department of Energy, and facilities subject to regulation by the Nuclear Regulatory Commission (NRC).

Question: Are anti-risk, anti-vulnerability, or security measures that a facility takes incorporated into the risk tiering process? If not, does it discourage high risk chemical facilities from increasing security at their facilities and making them stronger?

Response: Facilities are never discouraged from increasing security measures, and the inclusion of enhanced security measures may be necessary for approval of a facility's security plan. Security measures that reduce risk and mitigate vulnerabilities are incorporated into the facility's Site Security Plan or Alternative Security Program, and it is a requirement that these meet the applicable risk-based performance standards before the Department can approve an SSP or ASP.

Question#:	4
Topic:	ISCD's risk assessment approach 4
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: The current risk assessment program clearly needs a lot of work and will likely undergo further changes.

Does that mean facilities will need to go through the risk assessment process again?

Response: After recommendations are received from the peer review panel, ISCD will determine whether and/or which changes to the risk assessment process need to be made, including whether facilities will need to be re-assessed for risk.

Question: What impact will that have on the overall progress of the CFATS program and on the backlog?

Response: DHS cannot speculate on what impact any changes to the risk assessment process will have on the backlog. ISCD continues to move forward with reviewing, inspecting, and approving security plans and is working on increasing the pace of these activities.

Question#:	5
Topic:	ISCD's risk assessment approach 5
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: DHS has determined that some of the 40,000 facilities are no longer high risk because they removed chemicals of interest or reduced their holdings of these chemicals below the Appendix A threshold before DHS made its final tiering decisions. In past hearings, DHS has asserted that this constitutes one of the successes of the program.

How many facilities have actually removed chemicals of interest, or reduced their holdings below the threshold?

Response: Since the inception of CFATS, 3,083 chemical facilities have eliminated, reduced, or otherwise made modifications to their holdings of potentially dangerous chemicals and are now no longer considered high-risk.

Question: Does DHS verify that these chemicals have been removed or reduced? If so, how?

Response: Yes, the facility submits information to the Department through a revised Top-Screen and/or materials accompanying a Request for Redetermination. If the information is not sufficient, DHS may visit the facility to verify that the chemicals have been removed or reduced, or that processes have otherwise been modified.

Question#:	6
Topic:	ISCD's risk assessment approach 6
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: Do you plan to expand the scope of the CFATS program aside from eventually including economic consequences into the risk assessment approach?

If so, is this prudent given the challenges you have had implementing the currently scoped program?

Response: NPPD is committed to continued progress within the CFATS program. The Department is striving to ensure that all high-risk chemical facilities under CFATS have appropriate measures in place to address their security risks. In order to achieve this, the Department is exploring whether the current scope of the program is broad enough to include all non-exempted high-risk chemical facilities. I believe this is prudent in light of the importance of the CFATS mandate and the improvements the Department has made over the last year to the CFATS program, its management, and its operations.

Question#:	7
Topic:	site security plan review process 1
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: GAO says that ISCD has developed an operating plan to measure the performance of the CFATS program, and states that 63 measures are to track the site security plan review process, 9 are to track performance of ISCD's outreach efforts with industry.

Have you developed a new operating plan? If so, please provide it to the Committee.

What are some performance measures in the operating plan?

Does the plan include measures for aspects of the CFATS program other than the security plan review process and outreach efforts?

Considering the challenges ISCD has experienced with its information technology systems, will you be able to track data on these measures? Will the data tracked be reliable and useful?

How do you plan to use the data collected for each performance measure to improve CFATs program performance?

Response: ISCD developed an internal operating plan that was signed by the Director in December 2012. The Annual Operating Plan is an internal document, but the Department would be happy to provide a briefing to the Committee on this topic and discuss performance measures.

Question#:	8
Topic:	site security plan review process 2
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: GAO notes that it could take 7 to 9 years to review security plans.

Will you use alternate security programs to streamline the inspection process to alleviate the backlog?

Response: The Alternative Security Program (ASP) is one method for addressing the backlog. The Department is also exploring other options to reduce the backlog and to streamline the inspection process.

Question: Will these changes allow ISCD to approve plans and inspect facilities for compliance more quickly?

Response: We believe that the use of ASPs has the potential to significantly increase the pace at which we inspect and approve security plans. ISCD has been working closely with industry stakeholders regarding options for their development and use of ASPs. DHS has also been engaging industry on the development of "corporate" ASPs. For members of industry that own or operate several regulated facilities, the company can develop a company-specific ASP template that can be easily tailored to the specifics of each facility. This uniformity of approach across multiple facilities is likely to enable ISCD to review and, as appropriate, approve ASPs more quickly.

Question#:	9
Topic:	site security plan review process 3
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: The 2011 internal memo described a lack of training as a barrier to ISCD reviewing security plans and completing inspections.

Did this lack of training exacerbate the delay in reviewing site security plans?

Response: The SSP review process begins with an initial review to determine whether or not a facility's SSP should be authorized. After issuing a Letter of Authorization, ISCD conducts a comprehensive and detailed authorization inspection. The inspection results, as well as any further revisions that the facility may make to the SSP, are reviewed to make a final determination as to whether the facility's SSP satisfies the applicable RBPSs and whether to issue a Letter of Approval. Enhanced training, as well as process improvements, have greatly assisted ISCD in reducing the timeframes for each step in the process.

Question: How has ISCD changed its training program to ensure that staff are properly trained to review site security plans and conduct authorization inspections?

Response: ISCD has worked to standardize processes and develop training to coincide with these processes. Based on lessons learned during the first inspections, ISCD was able to develop a long-term inspections training program and administer this program to all Chemical Security Inspectors. In developing and delivering this training, ISCD focused on the key elements required to perform the inspection and ensured that personnel with the appropriate skill-sets and backgrounds were involved in developing and delivering the training.

Question: How are authorization inspections going?

Response: ISCD has increased the pace at which it conducts authorization inspections and has received positive feedback from industry stakeholders on the process and on the professionalism of the Chemical Security Inspectors. As of April 9, 2013, ISCD has completed 181 authorization inspections and has increased the pace of authorization inspections to approximately 50 per month.

Question: What types of things are inspectors finding at facilities?

Question#:	9
Topic:	site security plan review process 3
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Response: The Inspectors are noting the numerous security measures that facilities have in place, are identifying some gaps in security, and are discussing with facilities options for how to comply with CFATS. For example, during one authorization inspection, an Inspector identified an outdoor storage location for a chemical of interest that was not previously identified in the security plan. The facility indicated the cylinder containing the chemical of interest was difficult to move; therefore the facility did not think it was a security issue to store the chemical of interest outdoors with little to no protection. Upon further discussion, the Inspector helped the facility to realize the security risk this situation posed, as the gates to the facility were not secure and equipment was available onsite to transfer the heavy cylinder. The facility has now started the process of installing additional delay barriers and detection capability for this storage area.

ISCD is also finding that facilities' Site Security Plans are becoming more detailed and facilities are including new planned measures for security enhancements in order to achieve an approved Site Security Plan. ISCD is finding that facilities' Site Security Plans are much closer to receiving approval. As of April 9, ISCD has been able to issue 62 Letters of Approval.

Question#:	10
Topic:	site security plan review process 4
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: DHS established the CFATS program in April 2007 with the publication of the CFATS rule and has spent almost $500 million since then on the program. Now, GAO reports that it may take 7 to 9 more years for ISCD to review the security plans for facilities regulated by CFATS.

Based on your experiences seeing the program from day-to-day, what assurances do we have that committing additional resources to the CFATS program will result in a regulatory program that is fully functional and operating as Congress intended?

Response: Since the inception of CFATS in 2007, the Department has made significant progress implementing the program. More than 3,000 chemical facilities have eliminated, reduced, or otherwise made modifications to their holdings of potentially dangerous chemicals and are now no longer considered high-risk. In addition, the Department has:

- Developed and adopted a regulatory framework to address the security of chemical facilities that the Department determines pose high levels of risk.
- Published CFATS Appendix A, which identified 322 chemicals of interest and established a Screening Threshold Quantity for each chemical of interest based on its potential to create significant adverse consequences to human life or health.
- Developed the Chemical Security Assessment Tool (CSAT) to help NPPD identify potentially high-risk facilities and to provide methodologies those facilities can use to conduct Security Vulnerability Assessments and to develop security plans.
- Issued Risk-Based Performance Standards Guidance to assist final high-risk chemical facilities in determining appropriate protective measures and practices to satisfy the RBPS.
- Received data from more than 44,000 Top-Screens submitted by chemical facilities, providing important information about their chemical holdings.
- Identified more than 8,000 facilities that it has initially designated as high-risk. These facilities have used the CSAT tool to compile and submit Security Vulnerability Assessments.
- In May 2009, following reviews of facilities' Security Vulnerability Assessment submissions, ISCD began notifying facilities of their final high-risk determinations, tiering assignments, and the requirement to complete and submit a

Question#:	10
Topic:	site security plan review process 4
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Site Security Plan (SSP) or an Alternative Security Program (ASP) in lieu of an SSP.

- As of April 8, 2013, CFATS covers 4,365 high-risk facilities nationwide; of these, 3,442 have received final high-risk determinations and are required to develop SSPs (or ASPs) for DHS review. Of those facilities with final high-risk determinations, 4,257 have submitted SSPs (or ASPs). The remaining facilities are awaiting final tier determinations based on their Security Vulnerability Assessment submissions.

Over the past year, NPPD has worked diligently to turn a corner and has addressed many issues previously identified as challenges. The CFATS program has made significant progress, advancing programmatically while simultaneously addressing internal operational concerns. ISCD has committed permanent leadership who are focused on making the program a success. This is evident through the increased number of authorizations, inspections, and approvals to date.

Question#:	11
Topic:	outreach to facility owners and operators 1
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: Regulated owners and operators and other interested stakeholders have expressed dissatisfaction with the on-line, computerized tools used to complete various CFATS documents and data collection requirements because the tools can be a burden to complete and use.

GAO says that ISCD's Annual Operating Plan highlights plans to re-engineer the online tool to make it more efficient and effective. What steps has ISCD taken most recently to improve the online tools and what are the projected timeframes for upgrading the online tools?

Response: ISCD is currently conducting a series of focus groups to listen and learn from industry their perspectives about the online tools. The President's FY 2014 budget request, if enacted, would allow us to update the CSAT tool by the end of 2014, which is consistent with the ISCD Action Plan.

Question: GAO asked key trade associations to comment on the effectiveness of ISCD's outreach efforts and the usefulness and burden associated with the online tools, among other things. Has ISCD surveyed the regulated community and other interested stakeholders to solicit their opinions and comments regarding making improvements to the online tools?

Response: Through existing outreach efforts, ISCD has recorded industry feedback regarding the CSAT tool. ISCD is currently conducting focus groups to further listen and learn from industry their perspectives on how to improve the CSAT tool.

Question: Will the IT system enable you to capture and continuously update answers?

Response: At this time, facilities can edit or request the ability to make edits to their Site Security Plans, though the opportunity to do so is not continuous. The requirements for the IT system have not been finalized; however, the ability to capture and continuously update answers is being considered.

Question#:	12
Topic:	outreach to facility owners and operators 2
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: You told GAO officials that you will consider eliminating unnecessary data requirements when revising the online tools, but may continue to request the data—even if they are not used for risk tiering—because it may help facilities as they prepare their security plans.

Has ISCD examined the appropriateness and usefulness of information collected via the on-line tools?

Response: Yes, ISCD has examined the appropriateness and usefulness of the information collected online. We expect the CSAT focus groups will validate findings and provide requirements for the updated tool.

Question: What plans if any, have you made to reduce the amount of information collected during the data collection process?

Response: After we have recorded industry's perspectives on how to improve the CSAT tool and identified the changes we will be making to the CSAT tool, ISCD will assess whether the relevant instruments in the current Information Collection Requests (the approved document for ISCD to collect information from facilities) for the CSAT tool needs to be updated. ISCD will continue to strive to collect only data that contributes to the program's efforts to identify and foster security at high-risk chemical facilities and to reduce the burden on respondents.

Question#:	13
Topic:	outreach to facility owners and operators 3
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable John M. Shimkus
Committee:	ENERGY & COMMERCE (HOUSE)

Question: GAO says you do not systematically solicit feedback to assess the effectiveness of outreach efforts, and do not have a mechanism to measure the effectiveness of your outreach activities.

What are your plans to obtain feedback regarding outreach efforts, particularly with regard to increasing understanding of the risk-tiering approach; the risk-based performance standards and the online tools used to comply with CFATS requirements?

Response: The Department is committed to improving efforts to systematically solicit and document feedback on CFATS-related outreach activities. We agree with the GAO recommendation and we are exploring options to collect and document stakeholder feedback.

Question: Will all CFATS facilities be included in the feedback?

Response: The number of facilities impacted by the revised outreach plan cannot be decided until ISCD determines a path forward for implementing the GAO recommendation.

Question#:	14
Topic:	CFATS 1
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable Gregg Harper
Committee:	ENERGY & COMMERCE (HOUSE)

Question: What is the CFATS program doing to conduct ongoing data collection, monitoring, and analysis of the facilities under their purview?

Response: To begin the process of assessing whether a facility is high-risk and regulated under CFATS, the facility uses the web-based Chemical Security Assessment Tool (CSAT), to submit a Top-Screen to ISCD. Since we began collecting this information in 2007, ISCD now has data from more than 44,000 Top-Screens submitted by chemical facilities, providing important information about their chemical holdings. Based on the information received in the Top-Screens, ISCD identified more than 8,000 facilities that were initially designated as high-risk facilities potentially regulated by CFATS. These facilities then compiled and submitted Security Vulnerability Assessments, which are used by ISCD to identify which facilities present a terrorism risk that is sufficiently high to warrant the assignment of a final high-risk tier under CFATS.

After a facility receives a determination that it is high-risk, the facility must develop a Site Security Plan (SSP) to document the existing and planned security measures that satisfy the applicable Risk-Based Performance Standards (RBPS) under CFATS. Following a facility's development and submission of an SSP, ISCD conducts an authorization inspection that is tailored to review specific details within the facility's SSP. High-risk facilities also have the option of submitting an Alternative Security Program (ASP) in lieu of an SSP.

Following SSP or ASP approval, ISCD may conduct compliance inspections to ensure that the facility is adhering to all aspects of its approved SSP or ASP.

At any point during the CFATS process, if there is a change in the quantity or types of Chemicals of Interest at facility, it may be required to file a new Top-Screen. In addition, following ISCD's approval of a facility's SSP or ASP, CFATS requires the facility to complete and submit a new Top-Screen approximately two years after approval if the facility is tier 1 or 2 or approximately three years after approval if the facility is tier 3 or 4.

Question: How does the CFATS program define threat risk? Are there levels to this determination?

Response: The current CFATS program considers all three components of risk—

Question#:	14
Topic:	CFATS 1
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable Gregg Harper
Committee:	ENERGY & COMMERCE (HOUSE)

consequence, vulnerability, and threat—at various junctures throughout the process. DHS is currently working to identify ways to further improve the phase of this process that assign high risk facilities to one of four tiers.

Question: Can you discuss why it will require an additional 18 months to complete the economic impact assessments that will be studied by Sandia National Laboratories? Are there other options available to the CFATS program in order to conduct initial economic impact assessments more quickly? What are the parameters of these assessments, and how can CFATS work to deliver useful data and risk analysis to this committee and to the leadership at the Department of Homeland Security?

Response: The Sandia National Laboratories Statement of Work has an 18 month period of performance. A report is expected in March 2014, but ISCD expects to receive interim reports throughout the period of performance. The Department has also asked the external peer review to provide comments on economic criticality/consequence if appropriate. The draft report from the peer review panel is expected in September 2013. The Department has engaged Sandia National Laboratories to assist in developing a model for identifying and tiering high-risk chemical facilities that includes economic consequences. When the Department receives reports from Sandia National Laboratories and the external peer review, we plan to engage the Committee to provide appropriate updates.

Question#:	15
Topic:	CFATS 2
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable Henry Waxman
Committee:	ENERGY & COMMERCE (HOUSE)

Question: At the hearing, you expressed support for the existing risk analysis model employed within the CFATS program, which does not include vulnerability as an element of risk and does not account for economic consequences. When asked whether the CFATS risk assessment should be consistent with the National Infrastructure Plan, you answered that, generally speaking, it should. But the findings of the Government Accountability Office show that the risk model is not currently consistent with the National Infrastructure Protection Plan or the Interim Final Rule that established the Chemical Facilities Anti-Terrorism Standards program.

Does DHS intend to modify the risk model to comport with the National Infrastructure Protection Plan and the CFATS rule, by incorporating vulnerability and other aspects of risk?

Response: The current CFATS program considers all three components of risk—consequence, vulnerability, and threat—at various junctures throughout the process. ISCD has engaged the Homeland Security Studies and Analysis Institute (HSSAI) to conduct an external peer review of the tiering methodology. The review commenced in February. The panel is comprised of eight members with expertise in risk analysis, infrastructure/industrial security, toxicology, chemical process safety, and chemical intelligence. We expect the peer review to provide recommendations on how DHS can enhance the CFATS tiering model as appropriate.

Question: If not, does DHS intend to revise the CFATS rule to comport with the risk model used in the program?

Response: Following receipt of the panel's recommendations, and depending on the changes that may need to be made to the current risk assessment process, we will evaluate whether additional modifications to the rule may be required.

Question: What is the timeframe for completing the expert panel review of the risk assessment model, responding to the recommendations in the National Academies report on DHS risk assessment, and carrying out the verification and validation recommended by GAO?

Response: The Department expects to receive the report from the external peer review panel in September 2013. After ISCD receives the peer review panel report, a

Question#:	15
Topic:	CFATS 2
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable Henry Waxman
Committee:	ENERGY & COMMERCE (HOUSE)

determination of next steps, including how to carry out the verification and validation recommended by GAO, will be made.

Question#:	16
Topic:	CFATS 3
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable Henry Waxman
Committee:	ENERGY & COMMERCE (HOUSE)

Question: The number of facilities that have reduced their chemical holdings and are no longer tiered is often cited as a measure of the success of the CFATS program. In your written testimony, you cited "close to 3,000" facilities that have eliminated, reduced, or modified their chemical holdings to reduce their risk and avoid falling within the CFATS program.

What is the exact number of facilities?

Response: Since the inception of CFATS, 3,083 chemical facilities have eliminated, reduced, or otherwise made modifications to their holdings of potentially dangerous chemicals and are now no longer considered high-risk.

Question: Please provide the Committee with the list of those facilities, as well as a characterization of the types of facilities that have made this change.

Response: Due to the sensitive nature of this information, the documentation will be provided to the committee under separate cover.

Question: Please provide the Committee with documentation received from those facilities to demonstrate the reduction in their holdings, as well as examples of safer chemicals, processes, or methods employed by those facilities to reduce their chemical holdings.

Response: The information submitted to the Department includes documentation such as bills of lading and receipts. Given the large number of facilities that have submitted information and the type of information received, the Department will follow up with the Committee regarding the feasibility of providing this documentation to the Committee. We feel that it might be best if we initially provide you with detailed briefings on the available documentation.

Question#:	17
Topic:	FOIA
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable Henry Waxman
Committee:	ENERGY & COMMERCE (HOUSE)

Question: I understand that the Department has denied FOIA requests for a list of the facilities that have reduced their holdings and are no longer tiered, as well as documentation on the changes in chemicals, processes, or methods that made this possible. The shift away from significant chemical holdings has been one of the main measures of success cited for this program, so it is important for this Committee and the public to understand what it really means.

Can you explain why the Department been unwilling to release the list of facilities that have taken action to substantially reduce their risk?

Response: DHS's denial of the referenced FOIA request is based on concerns that disclosure of the list could frustrate program effectiveness and impact public safety. This denial is currently under appeal. The Department would be willing, however, to brief the Committee on the list of facilities that have reduced, removed, or modified their chemical holdings to reduce their risk tier.

Question#:	18
Topic:	CFATS 4
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable Henry Waxman
Committee:	ENERGY & COMMERCE (HOUSE)

Question: The GAO and officials at the Department have reported on the development of a new strategic communication plan for the CFATS program.

Will this plan include systematic outreach for workers at facilities determined to be high risk?

Response: The strategic communications plan may include systemic outreach to facilities, including employees at the facilities. The specifics will be determined during the development of the plan.

Question: Will the plan include informal outreach for workers? Does any such informal outreach currently occur?

Response: The strategic communications plan may include informal outreach to facilities, including employees at the facilities. The specifics will be determined during the development of the plan. Informal outreach currently takes place through interaction between inspectors and some workers during Compliance Assistance Visits or Inspections.

Question: Will the strategic communication plan include outreach for communities around high risk facilities?

Response: The plan may include targeted outreach to public safety officials (including police departments, fire department, and other emergency responders,) in communities around high-risk facilities and outreach to the general public.

Question: Will ordinary people have any way of knowing that a facility down the street from their home puts them at risk?

Response: Information about whether or not a facility is considered high-risk is sensitive information from a security perspective. The Department does not disclose this information about high-risk chemical facilities to the general public. However, under other state, local, and Federal requirements, information about nearby chemical facilities may be available to members of the public.

Question#:	19
Topic:	CFATS 5
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable Henry Waxman
Committee:	ENERGY & COMMERCE (HOUSE)

Question: A suggestion was made during the hearing that facilities placed in tiers 3 and 4 may not merit regulation under the CFATS program.

Generally speaking, what might the impacts be of a successful attack on a tier 3 or tier 4 facility?

Response: A successful attack on a tier 3 or tier 4 facility could be highly damaging and similar in nature to an attack on a tier 1 or tier 2 facility, though with less resulting loss of life. While tiers 1 and 2 facilities represent the highest of the high-risk facilities, the risk at tiers 3 and 4 is considerable.

Question#:	20
Topic:	CFATS 6
Hearing:	The Chemical Facilities Anti-terrorism Standards (CFATS) Program: A Progress Update
Primary:	The Honorable Henry Waxman
Committee:	ENERGY & COMMERCE (HOUSE)

Question: When the Committee drafted H.R. 2868 in the 111th Congress, several provisions were included to guide the tiering process for CFATS facilities. Section 2102 of the bill directed the Department of Homeland Security to first make a list of high risk facilities, based on a consideration of threat and consequences, including adverse effects to human health, the environment, critical infrastructure, public health, homeland security, national security, and the national economy, as well as the geographic proximity to large population centers. Facilities on the list would then be sorted into tiers by the Department based on risk. Under this two step process, vulnerability would be considered in assessing risk and placing a facility into a tier, but not in determining whether a facility fell within the universe of CFATS regulated facilities.

By removing vulnerability from the threshold determination of what facilities are covered by CFATS, would this two step approach have addressed the concern raised by David Wulf at the hearing that a facility could cycle in and out of the regulated universe by adding or removing security measures?

Response: DHS believes that its implementation of CFATS provides appropriate consideration to vulnerability after facilities have been placed in tiers. However, in addition to considering the forthcoming recommendations of the peer review panel, the Department is open to considering additional ideas from the Committee on how the current risk assessment methodology can be improved.

United States Government Accountability Office
Washington, DC 20548

April 23, 2013

The Honorable John Shimkus
Chairman
Subcommittee on Environment and the Economy
Committee on Energy and Commerce
House of Representatives

Subject: *Critical Infrastructure Protection: GAO Response to Posthearing Questions for the Record*

Dear Mr. Chairman,

On March 14, 2013 we testified before your committee on the actions the Department of Homeland Security (DHS) has underway to better manage its chemical security program,[1] and have subsequently issued a related report.[2] You requested that we provide additional information on a number of post hearing questions. The questions and our answers are provided in the Enclosure. The responses are based on work associated with previously issued GAO products. If you have any questions about this letter or need additional information, please contact me at (202) 512-9610 or CaldwellS@gao.gov.

Sincerely yours,

Stephen L. Caldwell
Director
Homeland Security and Justice

Enclosure

---

[1]GAO, *Critical Infrastructure Protection: Preliminary Observations on DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach*, GAO-13-412T (Washington D.C.: March 14, 2013).

[2]GAO, Critical Infrastructure Protection: *DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened*, GAO-13-353, (Washington, D.C.: April 5, 2013).

Enclosure

Questions from the Honorable John Shimkus

Infrastructure Security Compliance Division (ISCD) risk assessment approach

1. **Do you think the peer review should precede any amendments to the Chemical Facility Anti-Terrorism Standards (CFATS) regulations or expansion of the list of chemicals of interest?**

   In a report issued subsequent to our testimony before this Subcommittee, we recommended that DHS conduct an independent peer review, after ISCD completes enhancements to its risk assessment approach that fully validates and verifies the approach.[3,4] However, we did not examine whether a peer review should precede any amendments to the rule or an expansion of the list of chemicals of interest. As we have previously reported, independent peer reviews cannot ensure the success of a risk assessment approach, but they can increase the probability of success by improving the technical quality of projects and the credibility of the decision-making process.[5] Commissioning an independent peer review—including a complete verification and validation of the models used to tier facilities—following DHS actions to revise and enhance its risk assessment approach might better inform any changes to the rule and the list of chemicals of interest included in Appendix A.

2. **Given that past evaluations did not disclose problems with the current model, will the peer review be in a better position to identify potential problems? Why?**

   Once the panel of subject matter experts completes its ongoing examination of the current risk assessment approach, ISCD may have a better understanding of the current approach's strengths, weaknesses, and whether ISCD is heading in the right direction when tiering facilities. After the panel of experts recommendations are incorporated into the risk assessment approach, the peer review is to include steps that are to independently validate and verify the CFATS risk assessment approach, such as analyzing the structure of the approach and determining whether the risk models included in the approach calculate values correctly. By including these validation and verification steps, ISCD should be better positioned to identify any additional potential problems with the CFATS risk assessment approach.

---

[3]GAO, *Critical Infrastructure Protection: Preliminary Observations on DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach*, GAO-13-412T (Washington D.C.: March 14, 2013).

[4]GAO, Critical Infrastructure Protection: *DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened*, GAO-13-353, (Washington, D.C.: April 5, 2013).

[5]See GAO-12-14 and GAO, *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T (Washington D.C.: Mar. 31, 2004).

ISCD security plan review process

3. **How does ISCD's problems implementing CFATS jeopardize its ability to effectively assess facility risk including reviewing site security plans and regulate and work with the chemical industry?**

   We identified three factors that could affect program operations and jeopardize ISCD's ability to implement an operational CFATS regulatory regime. First, the risk assessment approach is not yet complete because it does not consider all elements of risk called for by the National Infrastructure Protection Plan (NIPP) and the CFATS rule. Until ISCD incorporates all elements of risk into its risk assessment approach, ISCD will not know if it is regulating all of the facilities that pose the greatest risk or conversely, regulating facilities that should not be included in the program.

   Second, ISCD has increased the number of security plan approvals and attributes this increase to changes in the security plan review process. However, ISCD is unable to measure how these changes have affected the review process because ISCD did not track data on prior processes. Moving forward, ISCD plans to measure the time it takes to review plans, among other things, but it will not be able to fully measure progress until the new security plan review process matures. Tracking the time it takes to review security plans would enable ISCD to identify any problems and, where appropriate, take corrective actions.

   Third, ISCD currently does not solicit or collect feedback in a systematic fashion on its industry outreach efforts so that the effectiveness of these efforts can be measured. By not doing so, ISCD may be missing opportunities to improve its interactions with the chemical industry. Also, soliciting systematic feedback could help ISCD identify any emerging issues associated with implementing CFATS so that it could address potential problems before they occur.

4. **ISCD told you that it has efforts underway to expedite the review of the backlog of security plans. Will these efforts clear the backlog more quickly?**

   In March 2013, ISCD began actively exploring how the security plan review process might be expedited, such as potentially leveraging alternative security programs, reprioritizing resources, and streamlining review and inspection requirements. Since ISCD only recently began exploring these efforts, it is too early to tell whether these efforts will result in the expedited review of security plans.

5. **Could you comment on the documentation issues regarding the CFATS risk tiering approach? Does this lack of documentation impact the Department of Homeland Security's (DHS) ability to appropriately tier high risk chemical facilities?**

   The effect of the lack of documentation on DHS's ability to appropriately tier facilities the CFATS risk tiering may not be known until the efforts of the ongoing expert panel and the aforementioned independent peer review are completed. It is possible that the lack of documentation could hinder the ongoing expert panel and independent peer review in their efforts to review the CFATS risk assessment approach because participants will not have the benefit of knowing how and why decisions about the design and structure of the approach were made during the early years of the program.

ISCD outreach to owners and operators

6. **Would a systematic approach to soliciting feedback on ISCD's outreach efforts and progress improve the CFATS program?**

   Consistent with our recommendation that ISCD explore opportunities and take action to systematically solicit and document feedback on facility outreach, systematic efforts to solicit feedback from the regulated community might provide ISCD with an opportunity to determine if problems exist, not only with outreach efforts, but also within the broader CFATS program as well. Feedback solicited from regulated facility owners and operators and industry stakeholders might also allow ISCD to make specific changes to outreach activities and also address any problems identified with CFATS operations in general. For example, we suggested in our report that ISCD could solicit feedback as a part of after-action reviews conducted at assistance visits, meetings and presentations and work with trade associations or other representatives of the regulated community to design and conduct member surveys. Feedback solicited through these mechanisms might better position ISCD to identify programmatic issues experienced by regulated facilities, create an opportunity for discussion of these issues and highlight potential changes and take corrective actions, if necessary, to address the problems identified.

Questions from the Honorable Henry A. Waxman

The Government Accountability Office's written testimony examined the Department of Homeland Security's outreach to facility owners and operators as well as some stakeholders, such as state and local governments and trade associations. Outreach to other stakeholders was not described.

1. **In your review, did you find formal outreach or communication with stakeholders in the public interest community, such as labor or environmental groups?**

2. **Did you find formal outreach or communication with workers at covered facilities, or their representatives?**

3. **Did you find formal outreach or communication with residents or community leaders around these facilities?**

4. **Did you find informal outreach with any of the above mentioned groups?**

   The scope of our work was limited to assessing ISCD's outreach to selected chemical industry trade associations and their members and as such, we did not review the extent to which the agency took action to provide outreach to the stakeholder communities beyond the trade associations and their members. The industry trade associations highlighted in our review were selected because ISCD interacts with these organizations on CFATS issues, among other things, and because these associations represent a large number of regulated facility owners and operators in the program. ISCD data on outreach activities performed from fiscal year 2007 through the first quarter of fiscal year 2013 did not provide sufficient detail to determine whether formal or informal outreach or communication was performed with other stakeholder communities, such as labor and environmental groups and residents and community leaders around these facilities.

In the GAO's written testimony on the Department's forthcoming strategic communications plan, the Department's efforts are compared to other "customer service efforts in the government" suggesting that, "those receiving services can provide helpful information as to the kind and quality of services they want." The service provided by the CFATS program is a guarantee of security, and those receiving that service include workers in high risk facilities and people living around them.

5. **Based on your review, does the Department view those workers and residents as customers of the CFATS program?**

6. **Taking those groups as the customers of the CFATS program, how do the Department's communication efforts compare to other customer service efforts in the government?**

   The scope of our work was limited to assessing ISCD's outreach by obtaining views from selected chemical industry trade associations and their members. Thus, we did not examine whether DHS views workers in high risk facilities and the people living around them as customers of the CFATS program nor did we compare ISCD's communications efforts with those of other customer service efforts in the federal government. Furthermore, ISCD data on its outreach efforts did not provide the level of specificity that would enable us to determine if, or to what extent, ISCD's outreach efforts included workers at high-risk facilities or

residents living around them as customers. For example, ISCD data showed that outreach efforts included meetings at CFATS regulated facilities; presentations at federal, state, local, or private industry events; and meetings with federal, state, local, or private industry partners.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

April 4, 2013

Mr. Bill Allmond
Vice President
Society of Chemical Manufacturers
and Affiliates
1850 M Street, N.W., Suite 700
Washington, D.C. 20036

Dear Mr. Allmond:

Thank you for appearing before the Subcommittee on Energy and Power on Thursday, March 14, 2013, to testify at the hearing entitled "The Chemical Facility Anti-Terrorism Standards Program – A Progress Update."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Thursday, April 18, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Nick.Abraham@mail.house.gov and mailed to Nick Abraham, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

John Shimkus
Chairman
Subcommittee on Environment and the Economy

cc: The Honorable Paul Tonko, Ranking Member,
Subcommittee on Environment and the Economy

Attachment

July 15, 2013

Nick Abraham
Legislative Clerk
Committee on Energy and Commerce
2125 Rayburn House Office Building
U.S. House of Representatives
Washington, DC 20515

Re: Responses to Questions for the Record for "The Chemical Facility Anti-Terrorism Standards Program – A Progress Update" (March 14, 2013)

Dear Mr. Abraham:

SOCMA appreciates the invitation to testify at the above-referenced hearing before the Subcommittee on Environment & the Economy. We are pleased to provide the following responses to the Members' questions for the record. We apologize for the delay in our response.

The Honorable John Shimkus

1. **Do you think that ISCD is making progress with personnel surety? Is it headed in the right direction?**

A week after the hearing, DHS published a new information collection request (ICR) in connection with the CFATS personnel surety program (PSP).[1] In the almost two years since the previous ICR, ISCD engaged in significant outreach to the CFATS regulated community, which SOCMA appreciates. To some extent, that outreach has resulted in improvements to the program:

- *Limitation to Tiers 1 and 2.* Most important, ISCD has announced that it will limit the PSP for now to Tiers 1 and 2, and would publish another ICR before applying PSP to facilities in Tiers 3 and 4. This is a substantial improvement, as most affected SOCMA member facilities are in Tiers 3 and 4. This approach would allow ISCD to evaluate the implementation of the PSP at riskier facilities, and see what lessons can be learned from the experience, before the burdens of the PSP are imposed on lower-risk facilities.
- *Innovative monitoring alternatives.* The new ICR also announced that facilities may propose innovative alternatives such as video monitoring. Smaller facilities are especially unlikely to have free employees available to escort uncleared

[1] 78 Fed. Reg. 17680 (March 22, 2013).

visitors. The ability to use existing, centralized or stationary security personnel to provide "virtual escorting" would make the PSP far less disruptive for many facilities.

While these changes reflect progress, SOCMA remains concerned about two aspects of the PSP:

- *Requiring 48 hours prior notice*. The current ICR never discusses the issue, but it makes clear that DHS expects facilities to submit information for covered individuals 48 hours before giving them unescorted access to restricted areas or critical assets. Chemical facilities frequently have important contractors and visitors arriving upon short or no notice. Such people may have to come on site unexpectedly – for example, if a production unit goes down or otherwise requires emergency maintenance. A requirement that the facility know the identity of the particular individuals who will or may be arriving at the plant in advance would impose a substantial burden. Facilities would also likely suffer collateral or indirect effects from not being able to clear someone as quickly as he or she is needed. Conceivably, a production unit might have to be shut down because it could not be repaired before the requisite minimum prior notice period expired
- *Requiring PSP for individuals possessing TWICs or similar credentials*. The performance standard driving the PSP – Risk Based Performance Standard (RBPS) #12 – is that regulated facilities "[p]erform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including . . . [m]easures designed to identify people with terrorist ties."[2] DHS currently issues roughly a half-dozen credentials that require, as a condition of issuance, that DHS check the applicant against the Terrorist Screening Database (TSDB) – most notably including the Transportation Worker Identification Credential (TWIC) and the Hazardous Materials Endorsement (HME) to a commercial drivers license. Moreover, DHS recurrently vets these credentials against the TSDB so that it will discover if a credential holder subsequently has been added to the TSDB. In our considered view, a facility has satisfied its obligation under RBPS #12 if it determines that an individual possesses one of these credentials. We believe DHS does not have authority to require such individuals to be subjected to the PSP, which will only increase delays at facilities and raise implementation costs.

2. How does the recent experience of the regulated community with the CFATS program compare with its experience at the time of the Subcommittee's last hearing on September 11, 2012? Are there improvements and, if so, what are they?

Under David Wulf's leadership, the CFATS program has continued to improve since last fall:

---

[2] 6 C.F.R. § 27.230(a)(12).

- Most important, ISCD continues to inspect and authorize an increasing number of facilities, and has begun inspecting Tier 2 and 3 facilities.
- ISCD also announced approval of an Alternative Security Program, developed jointly by ISCD and the American Chemistry Council (ACC) but available to any CFATS-regulated facility. ISCD's endorsement of the ASP has enormously simplified the process of developing a Site Security Plan (SSP) and has greatly shortened the time it takes ISCD to conduct an authorization inspection.
- SOCMA members' interactions with ISCD inspectors have also continued to improve. Inspectors are providing sufficient details with facilities prior to their arrival onsite, including an itinerary for their visit, which greatly assists facility personnel in planning ahead for the inspector to ensure resources and personnel are available if needed. The amount of time spent by inspectors onsite conducting the facility is also reasonable, with some inspections only taking two to three days. Last, but highly important, inspectors appear no longer to be adhering rigidly to the RBPS Guidance and, instead, are permitting company personnel to explain, from the facility perspective, how they are appropriately implementing their site security plan. On the other hand, and as noted in our testimony, inspectors should give facilities more than the customary 30 days DHS requires now to resubmit revised SSPs following an authorizing inspection (AI). DHS should put in writing explicit consideration of extended time, preferably up to 90 days, for facilities, when requested and on a case-by-case basis, to resubmit revised SSPs. We have heard from at least one SOCMA member that requested from their inspectors more time at the end of an AI and were told by the inspectors that they can request extra time but that they should not expect to be granted it. If ISCD develops a process to consider extra time for facilities, ISCD needs to ensure that its inspectors are fully aware of the process and to ensure requests are considered fairly and transparently.

3. **What is the quality of communication between DHS and the regulated community? Is feedback systematic or based more on occasional, informal contacts?**

DHS and the regulated community interact predominantly through bi-monthly meetings of the Chemical Sector Coordinating Council (CSCC) with ISCD leadership and other DHS officials. We occasionally will meet or have conference calls more frequently as needed. We are generally pleased with this arrangement.

4. **Should feedback from the regulated facilities be more systematic through direct, detailed surveys? Would this significantly improve CFATS?**

SOCMA questions whether regulated facilities would appreciate being regularly surveyed regarding CFATS – such surveys could be distracting and burdensome. (The survey would have to be approved under the Paperwork Reduction Act, a process that would create its own demands on DHS and the regulated community.) We are also not

confident how good the response rate to such surveys would be, for the same reason. In general, we believe that the current system works optimally – member companies of the trade associations that make up the CSCC are able to surface concerns within their associations, and those associations can raise those concerns with DHS individually or via the CSCC.

5. **Overall, both DHS and GAO agree that there is progress on communication with the regulated community – do you think DHS has enabled you to fully understand the CFATS program and how DHS arrives at decisions?**

As a general matter, that depends:

- We feel that we do understand how the DHS evaluates SSPs and conducts inspections.
- Sometimes we understand how DHS makes policy decisions regarding the CFATS program – some explanations are more opaque than others.
- We have very little idea how facilities are tiered, since DHS has classified the methodology and does not explain to facilities why they were tiered as they were. We have generally had the impression that CFATS has gone overemphasized or overweighted the theft and diversion scenario, in effect tiering chemicals, not facilities. Now we see why: DHS has not been taking threat into account for the theft and diversion scenario, and it has not been considering vulnerability for *any* scenario. We look forward to the outcome of the ongoing peer review of the tiering methodology, and hope that it will include some amount of validation or verification of the methodology, rather than just looking at the model documentation.

We believe that DHS should explain to facilities why they were assigned to particular tiers, and where facilities have personnel with security clearances, DHS should explain precisely how the facility was evaluated by the tiering methodology. We note that Section 9(c) of the recent Executive Order on critical infrastructure cybersecurity (EO 13636[3]) says that, when DHS determines that a particular entity is "greatest risk," it will "ensure identified owners and operators are provided the basis for the determination." This is a serious due process issue, and DHS should address it.

The Honorable Henry A. Waxman

1. **Do SOCMA members support the consideration of vulnerability in determining the risk tier assignment for a facility, as set out in the National Infrastructure Protection Plan and the Interim Final Rule that created the CFATS program?**

[3] Available at http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Yes. By statute, CFATS must be a risk-based program,[4] and the security risk posed by facility is a function of threat, vulnerability and consequences. All three factors must therefore be considered by DHS in tiering facilities.

2. **Do SOCMA members support the two-step process set out in H.R. 2868, so that only threat and consequence would be considered in making the determination of whether a facility is subject to the CFATS regulations?**

No. SOCMA believes that Congress got it right in 2006 and that chemical facility security should continue to be based on risk.

3. **Do SOCMA members support requirements to provide [the reason for a facility's tier assignment and, upon request, information related to the criticality of the facility] to the owners of operators of covered facilities?**

Yes. As noted in our response above to Chairman Shimkus' question # 5, we believe that this presents a serious due process issue. DHS should explain to facilities why they were assigned to particular tiers, and where facilities have personnel with security clearances, DHS should explain precisely how the facility was evaluated by the tiering methodology. Such an explanation should actually help facilities to reduce risk more effectively than at present, because it would allow them to see exactly which changes would most significantly reduce the risk estimated by the tiering methodology. We note that Section 9(c) of the recent Executive Order on critical infrastructure cybersecurity (EO 13636[5]) says that, when DHS determines that a particular entity is "greatest risk," it will "ensure identified owners and operators are provided the basis for the determination." DHS should do likewise under CFATS.

4. **Is there additional information that SOCMA members would want to receive with their tier assignment to increase transparency and accountability in the tiering process?**

Facilities should receive the specific items of information that were considered by the tiering methodology (or DHS staff) in determining the proposed tiering, and the methodology (or at least access to the tiering model interface) so that the facility can determine what tier level would be associated with particular changes at the facility.

---

[4] *See* Pub. L. 109–295, title V, § 550(a), 6 U.S.C. § 121 note ("[T]he Secretary of Homeland Security shall issue interim final regulations establishing *risk*-based performance standards for security of chemical facilities . . . . [S]uch regulations shall apply to chemical facilities that, in the discretion of the Secretary, present high levels of security *risk*. . . .") (emphasis added).

[5] *See* note 3 *supra*.

5. **Do SOCMA members support increasing transparency and predictability in the CFATS regulatory process through the establishment of specific deadlines for the submission of information describing material modifications to facility operations?**

The current CFATS regulations already require facilities to submit a revised Top-Screen within 60 days of making a material modification. *See* 6 C.F.R. § 27.210(d).

The problem associated with material modifications during the early years of the CFATS program was that facilities that experience frequent changes in the presence or quantity of a chemical of interest or in site configurations were being required to submit multiple revised Top-Screens, often well before DHS had responded to prior submissions.

6. **Are all MSTA facilities owned and operated by SOCMA members implementing security measures sufficient to meet the CFATS tier 1 standards?**

SOCMA does not know the answer to this question. SOCMA member companies are required to implement ChemStewards, an environment, health, safety and security performance improvement program that includes external third-party verification. ChemStewards includes a requirement that facilities not in the CFATS program implement a security vulnerability assessment and implement security countermeasures commensurate with assessed risks. Thus SOCMA member facilities regulated under MTSA may well have adopted security measures that go beyond what MTSA requires.

7. **Do SOCMA members support requiring MTSA regulated facilities to meet security standards equivalent to the standards applicable to the tier such facilities would be assigned to if covered by the CFATS program?**

SOCMA would have a number of concerns with this approach. First, the Coast Guard has done a good job of standing up the MTSA program and administering it. We question the extent to which the Coast Guard currently has the resources and personnel to in effect superimpose CFATS onto the MTSA program. We suspect that the Coast Guard does not support that change. Second, we would be concerned about transposing to the MTSA program the identified flaws in the CFATS tiering process. Third, we would oppose any program under which ISCD was authorized to overrrule or redirect the Coast Guard with respect to MTSA facilities. Each component should remain independent of the other.

8. **How many facilities owned or operated by SOCMA members have reduced their chemical holdings to "tier-out" of the CFATS program?**

We have never attempted to gather this information systematically from our membership. Anecdotally, a sizable percentage of the SOCMA member company facilities that completed a Top-Screen have since exited the CFATS program.

9. **What chemicals, processes, or technologies, have those facilities used to reduce their holdings of substances of concern?**

Again, we have never attempted to gather this information from our members. In many cases, our members would regard that information as having competitive value and would not want to share it.

Thank you once again for the opportunity to respond to these questions. If you have any questions about them or need any further information, please do not hesitate to contact me at 202-721-4122 or allmondb@socma.com.

Sincerely,

William E. Allmond, IV
Vice President, Government and Public Relations

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

April 4, 2013

Mr. Timothy J. Scott
Chief Security Officer
The Dow Chemical Company
P.O. Box 156
Lake Jackson, TX 77566

Dear Mr. Scott:

Thank you for appearing before the Subcommittee on Energy and Power on Thursday, March 14, 2013, to testify at the hearing entitled "The Chemical Facility Anti-Terrorism Standards Program – A Progress Update."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Thursday, April 18, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Nick.Abraham@mail.house.gov and mailed to Nick Abraham, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

John Shimkus
Chairman
Subcommittee on Environment and the Economy

cc: The Honorable Paul Tonko, Ranking Member,
Subcommittee on Environment and the Economy

Attachment

April 29, 2013

Mr. Nick Abraham
Legislative Clerk
Committee on Energy and Commerce
2125 Rayburn House Office Building,
Washington, DC 20515

Re: The Chemical Facility Anti-Terrorism Standards Program – A Progress Report

The American Chemistry Council (ACC) appreciates this opportunity to respond to members of the Committee regarding the recent oversight hearing on March 14, 2013 before the Subcommittee on Energy and Power. Attached is our formal response to questions for the record. This response was prepared by ACC in conjunction with Mr. Tim Scott, Chief Security Officer with the Dow Chemical Company who testified on behalf of Dow and the ACC.

ACC commends the Committee for taking a strong leadership role and providing oversight on this important Chemical Security Program. While ACC believes that DHS has made progress, more work needs to be done. ACC stands ready to assist members of the Committee and DHS to improve the CFATS program and advance the state of chemical security across the Nation.

Regards,

Walter Moore
Vice-President, Federal Affairs

April 29, 2013

ACC Responses to Post Hearing Questions for the Record – March 14, 2013 "CFATS Program – A Progress Update"

The Honorable John Shimkus:

1. **Do you think that ISCD is making progress with personnel surety? Is it headed in the right direction?**

Since DHS withdrew its personnel surety program (PSP) proposal from the Office of Management and Budget (OMB) this past summer, DHS has done a commendable job in reaching out to stakeholders and incorporating many of the ideas that will help streamline the program and reduce burden on the regulated community. By leveraging existing programs, such as the Transportation Worker Identification Credential (TWIC), and by allowing for corporate and third-party submissions for vetting against the Terrorist Screening Database (TSDB), a significant reporting burden will be minimized, while the integrity of the program is maintained.

The goal of PSP is to ensure that personnel who have access to sensitive areas of high-risk chemical facilities do not pose a security threat to the facility, its workers or to the surrounding community. However, the current proposal may not provide the level of assurance necessary to ensure such threats are minimized. This is due to the fact that DHS has not provided any detail regarding their vetting procedures, including how and under what circumstances DHS will notify a facility that their personnel have been successfully vetted and how matches against the TSDB are resolved. It is crucial, that such personnel are vetted and cleared *prior* to being granted access to such sensitive areas. ACC believes that DHS must provide proper and timely notification to the covered facility that such persons have been vetted and are cleared for access *prior* to entry.

ACC is optimistic, given the changes made in this recent proposal, that a workable PSP is achievable. Until such time, however, no site security plans can be completely authorized or approved. We urge members of the Committee to address this important issue so that all high-risk chemical facilities are safe, secure and fully compliant with all 18 CFATS Risk Based Performance Standards.

2. **How does the recent experience of the regulated community with the CFATS program compare with its experience at the time of the Subcommittee's last hearing on September 11, 2012? Are there improvements and, if so, what are they?**

Since the last CFATS oversight hearing on September 11, 2012, ACC published its ASP Guidance Document for CFATS Covered Chemical Facilities. This document was the culmination of a year-long initiative including ACC, members of the regulated community and

DHS. Since then, we understand that several covered facilities have opted to submit an ASP in lieu of a SSP. Anecdotal reports from ACC members on the process indicate an improved clarity in compliance requirements and in conversations with DHS as a direct result of using the ASP.

Similar anecdotal reports from ACC members indicate that recent authorization inspections have been conducted in a far more efficient and effective manner, compared to prior inspections. The inspection staff is more knowledgeable, better trained and focused on specific compliance issues, requiring less time and manpower to cover the same material.

Communications between DHS and the regulated community have improved. This has been evidenced by the recent stakeholder engagement during the Personnel Surety Program (PSP) review leading up to their latest proposal. Additional, DHS has recently launched a series of focus group sessions around the country to gather feedback from the regulated community on ways to improve their suite of online CSAT tools. These sessions should provide DHS with the information and ideas that will greatly improve the effectiveness of the CFATS program.

Lastly, DHS has commissioned a third-party Panel Review of its Risk Tiering Methodology. This panel includes risk assessment experts as well as security and regulatory experts. In addition, members of the regulated community were given a chance to present their experiences with the risk tier process to the panel.

3. **What is the quality of communication between DHS and the regulated community? Is feedback systematic or based more on occasional, informal contacts?**

Depending on the nature of the issue, the feedback provided to DHS has been through both systematic and informal information sharing. For example, DHS has used a number of systematic approaches to collect input on various aspects of the CFATS program including focus group sessions, working groups, peer review and Federal Notices. Additional, DHS has increased its outreach to specific members of the regulated community, trade associations and with the Chemical Sector Coordinating Council.

4. **Should feedback from the regulated facilities be more systematic through direct, detailed surveys? Would this significantly improve CFATS?**

DHS could improve its ability to communicate with the CFATS regulated community as a whole, and feedback in all forms can be helpful to improve the CFATS program. Depending on the nature of the issue, a detailed survey might be the right approach. However, other forms of information collection may provide better data. For example, DHS does not seem to have the ability to send or collect information targeting the CFATS regulated community as a whole. The result is an uneven understanding about the current status of the program and compliance expectations.

5. **Overall, both DHS and GAO agree that there is progress on communication with the regulated community – do you think DHS has enabled you to fully understand the CFATS program and how DHS arrives at decisions?**

While DHS has made improvements in enabling the regulated community to more fully understand the CFATS program, more progress can be made. In particular, the process for assigning a risk tier to a covered facility is unclear and may produce incorrect results.

All factors used by DHS regarding the assignment of a risk tier for a CFATS covered facility are not shared with the facility. This lack of transparency between the CFATS process and the regulated facility continues to be a concern and is contrary to an effective security partnership. In the CFATS tiering process, the regulated facility is <u>not</u> made aware of the following factors:

- How information provided to DHS relates to their security posture or potential vulnerabilities at the facility level;
- How DHS analyzes site specific information provided by the facility;
- How tiering decisions are made;
- How changes made to the facility or to security practices will affect their risk level (tier)

The responsibility of the facility security manager is to understand the risks and vulnerabilities at his location and make prudent, well informed risk mitigation and security investment decisions. ACC recommends that, if requested by a covered facility, DHS should share all factors associated with their risk tier assignment. The covered facility should have the opportunity to engage DHS and provide information to ensure that the facility is being tiered properly and that facility security management is well informed and prepared to make important security decisions.

6. **GAO testified that it will take 7 to 9 years more to fully implement CFATS.**

April 29, 2013

ACC Responses to Post Hearing Questions for the Record – March 14, 2013 "CFATS Program – A Progress Update"

a. Could using Alternate Security Programs (ASPs) speed things up?

The ASP Guidance Document developed by ACC in conjunction with the regulated community and DHS provide the ability to increase the pace of CFATS implementation. The ASP initiative is an excellent example of how an effective public/private security partnership can create smart regulatory solutions that will benefit DHS, the regulated community and the surrounding community.

The DHS Site Security Plan (SSP) has been often identified as a roadblock in moving the CFATS program forward, which is a cumbersome process, marked with duplicative reporting and unclear questions regarding measures to minimize security risk at a covered facility. To overcome this, the ASP option provides a more efficient alternative.

ACC launched the ASP initiative in November of 2011with the goal of providing an effective option for CFATS facilities to develop and submit security plans in an efficient manner by minimizing duplication and reducing the effort required to properly assess and audit plans for approval. ACC worked with DHS and members of the regulated community for more than a year and in December of 2012 published the ASP Guidance Document and Template. Available for free to the public, the ASP Guidance Document and Template provides guidance on how to create an effective security plan for submission to DHS, which clearly demonstrates a facility's compliance with the 18 Risk Based Performance Standards (RBPS), while providing an operational plan that can be used by site personnel as well as DHS during an inspection.

While DHS has made progress in moving CFATS implementation forward, more needs to be done. Existing industry security programs, such as the ACC Responsible Care Security Code, should be recognized by DHS under their ASP authority as meeting initial hurdles for CFATS authorization, thus streamlining and prioritizing reviews. DHS would still be required to verify compliance by conducting a final site inspection. ACC believes this process could free up DHS resources so they can focus on those facilities and plans needing the most attention.

Another opportunity for efficiency is the "corporate review." Companies who have multiple CFATS facilities typically operate under a single corporate procedure for many of the Risk Based Performance Standards. Cybersecurity and site security escalation processes are two

common examples. Currently, CFATS inspections cover the same information, site-by-site, instead addressing the issue once at a corporate level. Corporate reviews can be utilized by DHS to cover issues once, reducing the redundancy and improving the pace of inspections.

b. Is there any security trade-off between a CFATS Site Security Plan and an ASP?

No, there is no security trade-off between an SSP and an industry ASP. The ASP does not change a covered facility's compliance obligations under the CFATS regime. If anything, an ASP provides a security benefit by providing a clearer more complete and understandable description of a site's security program and how it complies with the 18 Risk Based Performance Standards. In addition, the final product results in an "auditable operational document" that both the site security personnel, as well as DHS inspectors can use to inspect the facility for compliance. This is not the case with the conventional SSP.

The Honorable Henry A. Waxman:

1. **Do ACC members support the consideration of vulnerability in determining the risk tier assignment for a facility, as set out in the National Infrastructure Protection Plan and the Interim Final Rule that created the CFATS program?**

As discussed in question 5 above, DHS does not share all information related to the assignment of a risk tier with the covered facility, including vulnerability information. This lack of transparency between the CFATS process and the regulated facility continues to be a concern and is contrary to an effective security partnership.

Vulnerability assessment is a core element of an effective security risk management program. All members of the ACC are required to conduct security vulnerability assessments (SVAs) as part of their obligation under the ACC Responsible Care Security Code, which is requirement of membership. Results from the SVA provide the relevant information to address in their site's security plan. It also helps prioritize capital and security investments to those areas needing the most attention.

2. **Do ACC members support the two step process set out in H.R. 2868, so that only threat and consequence would be considered in making the determination of whether a facility is subject to the CFATS regulations?**

April 29, 2013

ACC Responses to Post Hearing Questions for the Record – March 14, 2013 "CFATS Program – A Progress Update"

Under CFATS today, facilities first need to submit information to DHS regarding security risk. This information may reflect potential consequences or vulnerabilities to a terrorist attack or incident. This includes, for example: information concerning the nature of the business and activities conducted at the facility; the names, uses storage conditions and other information concerning the chemicals at the facility; the facility's security, safety and emergency response practices, operations and procedures; and information concerning incidents, funding and other matters that bear on the effectiveness of the security, safety and emergency repose practices. After DHS receives this information, it is evaluated by DHS to determine if the information provided indicates the potential that a terrorist attack involving the facility could result in significant adverse consequences for human life or health, national security or critical economic assets. If the facility presents a high level of security risk, the facility is then placed in a risk-based tier.

After being placed in a tier, the facility must submit a security vulnerability assessment, which includes: the identification and characterization of critical assets; identification of hazards and consequences of concerns for the facility; a description of possible internal and external threats; identification of potential security vulnerabilities and effectiveness of existing countermeasures; an assessment of the degree of risk to the facility in terms of the expected effect on each critical assets and the likelihood of success of a terrorist attack; and an analysis of strategies that reduce the probability of an attack or the degree of success, and feasibility and effectiveness of such strategies. After review of this information, DHS makes a final decision as to which tier of risk the facility belongs.

ACC members believe that DHS should ensure that they effectively execute their mandate under CFATS. DHS must first conduct the detailed and methodical process to establish whether a facility is indeed a high risk facility and then determine what degree of risk is present, in accordance with the requirements set forth in CFATS.

3. **Do ACC members support requirements to provide that information to the owners and operators of covered facilities?**

ACC believes that DHS could provide better information to regulated facilities on their risk tier and compliance. ACC member companies are eager to implement CFATS in a timely fashion, including more rapid authorization inspections and plan approvals. While DHS has shown improvement in this area, particularly with the level of engagement by the DHS field inspectors, more needs to be done.

For example, DHS should leverage existing industry security programs such as the Responsible Care Security Code. Industry programs that require members to have a security management system in place and are audited by a certified third-party auditor could be used by DHS to help expedite some of the early CFATS authorization steps. This would help DHS focus their resources where they are needed most.

4. **Is there additional information that ACC members would want to receive with their tier assignment to increase transparency and accountability in the tiering process?**

ACC believes that DHS should be more forthcoming with the covered facility regarding all factors related to their risk-based tiering. The security manager at the site has the ultimate responsibility for the safety and security of its operations and he or she also has the authority to make informed risk mitigation and security investment decisions. Therefore, the information that the security manager needs to know in order to devise, implement and maintain an effective security program that addresses the risks at hand must be made available to the covered facility security manager. This issue is at the core of an effective security partnership.

5. **Do ACC members support increasing transparency and predictability in the CFATS regulatory process through the establishment of specific deadlines and requirements for the submission of information describing material modifications to facility operations?**

In order for industry to succeed, regulatory requirements must be clear and consistently applied by the agency. Standards need to be clear and compliance requirements need to be uniformly enforced. If a covered facility is engaged in a constant guessing game as to whether it is in compliance with the law, then money, time and effort may be needlessly wasted when it could be put to better use providing jobs, producing goods, or enhancing security and safety in new ways. If an agency is rushed to make a determination, the decision may not be based on a full evaluation of relevant information, and it may be flawed. An appropriate amount of time needs to be spent assessing all of the facts at hand, so the right regulatory determination can be made by the agency. ACC believes that DHS has to demonstrate that it has achieved this balance throughout the CFATS program, although there are aspects where it has performed better than others. ACC hopes that with time and with experience, DHS will be able to make timelier, well-reasoned, decisions in a fashion that provides industry with the predictability and certainty it needs to succeed.

6. **Are all ACC member companies implementing security measures at MTSA facilities sufficient to meet the CFATS tier 1 standards?**

Mr. Scott's testimony during the hearing was in response to an allegation made by a panelist that MTSA-regulated facilities in general and one specific Dow site were not adequately secured. Mr. Scott's response was specific to the Dow site that was mentioned and was speaking as the Chief Security Officer of The Dow Chemical Company.

Dow adopted and implemented the Responsible Care Security Code as it was first established by the American Chemistry Council, and implemented the Code on a global basis at all sites in order to achieve a consistent, global and corporate approach to our security programs and processes. Dow also conducted internal SVAs on a global basis. The Security Code includes a risk-based tiering process for sites. When CFATS and MTSA – along with other regulatory guidelines or requirements around the world – Dow complies with all regulations and uses the Security Code as a guideline for consistency when there are gaps in the risk assessment or tiering process or between the regulations. The risk-based performance standards developed by DHS were a good guideline to follow and implement in our corporate security guidelines and give us a consistent corporate approach while meeting the various government regulations. This is Dow's approach to globally integrated security program.

7. **Do ACC members support requiring MTSA regulated facilities to meet security standards equivalent to the standards applicable to the tier such facilities would be assigned to if covered by the CFATS program?**

The focus of the Chemical Facility Anti-Terrorism Standards and the Maritime Transportation Security Act are very different. CFATS is focused on physical attack on a manufacturing or storage facility, theft or diversion of chemicals for use as weapons, or insider threats that could cause a significant operational event at a site. MTSA is focused on the security of marine operations facilities and the movement of products to/from/through those marine operations. Both standards meet their intended purpose. While ACC does not support merging MTSA and CFATS programs, ACC has consistently supported the merging of appropriate aspects of these two programs as long as the merger improves efficiency and security without diluting the primary purpose of either program.

April 29, 2013

ACC Responses to Post Hearing Questions for the Record – March 14, 2013 "CFATS Program – A Progress Update"

8. **How many facilities owned or operated by ACC members have reduced their chemical holdings to "tier-out" of the CFATS program?**

ACC conducted a CFATS performance survey in the summer of 2011. When asked if their company had reduced the onsite quantity of any CFATS-regulated Chemical of Interest (COI), a majority of respondents said they had. For some respondents, their stated reason was purely for business purposes. For others it was to reduce their CFATS risk profile and/or reduce the number of facilities subject to CFATS regulation.

Chemical facilities routinely perform safety and security risk assessments for a variety of reasons including: compliance with federal, state and local laws; to remain competitive in the marketplace; to minimize insurance premiums; to protect workers and the community; to improve manufacturing efficiency and to reduce liability exposure. For whatever reason, the overall goal of a facility's risk management program is to produce products for the consumer market that improves the quality of life, provide safe employment for the community while minimizing their impact on the environment.

For members of the ACC, the Responsible Care Program requires regular assessments of security, safety and environmental risks and to minimize those risks through the implementation of measures, including the reduction of onsite chemical holdings.

9. **What chemicals, processes, or technologies, have those facilities used to reduce their holdings of substances of concern?**

The results of the ACC survey found that a majority of respondents regularly assess chemical alternatives or processes to reduce their risks. For those who were able to reduce their holdings, some consolidated their chemical holdings at one location. Others changed the way they conducted business, allowing them to maintain smaller inventories on-site (just in time production). In many cases, the technical feasibility or cost associated with process changes made it impractical. Potential risk-shifting was also noted as reason that limited their reduction of onsite chemicals, in the case of increased shipments. Lastly, product quality/customer specifications were another limiting factor.

Charles T. Drevna
President

American
Fuel & Petrochemical
Manufacturers

1667 K Street, NW
Suite 700
Washington, DC
20006

202.457.0480 office
202.552.8457 direct
202.457.0486 fax
Cdrevna@afpm.org

April 23, 2013

The Honorable John Shimkus
Chairman
U.S. House Subcommittee on Environment and Economy
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Shimkus:

AFPM appreciated the opportunity to provide its perspective during the March 14th, 2013 hearing entitled "the "Chemical Facility Anti-Terrorism Standards (CFATS) Program – A Progress Update." AFPM also appreciated the opportunity to address several questions submitted for the record.

Please feel free to contact me or my staff, Suzanne Gillen at (202) 457-0480 or sgillen@afpm.org with any questions. Again, thank you for the opportunity to share AFPM's views.

Regards,

Charles T. Drevna

The Honorable John Shimkus

1. **Do you think that ISCD is making progress with personnel surety? Is it headed in the right direction?**

No. AFPM members still have several concerns that need to be addressed on personnel surety. Congress intended that the Risk-Based Performance Standard 12 on Personnel Surety allow facilities the flexibility to determine the most efficient manner to meet the standard. Instead, DHS again proposed a personnel surety program stating how the regulated facilities are expected to meet the standard. AFPM recommends that DHS follow Congressional intent and personnel surety should be written as a risk-based performance standard.

There are still several issues that need to be addressed on personnel surety:

- **Submitting additional PII for federally vetted individuals is burdensome:** Facilities should have the option to use already established federally secure vetting programs, such as the Transportation Worker Identification Credential (TWIC), to satisfy CFATS without also submitting additional personally identifiable information (PII) to DHS. Submitting additional PII, such as a name, contact information, and date of birth, would be burdensome and unnecessary given that this type of information would already be submitted for previously vetted individuals and not further enhance security. AFPM appreciates that DHS has made an improvement to recognize the TWIC if it is verified with a reader. However, this is still a burdensome requirement for owners and operators of a facility to submit PII on individuals if a TWIC reader isn't used to verify the TWIC even if the individual is already federally vetted. If the goal is to lessen the burden and improve the process for those individuals who are already federally vetted, then DHS should allow for the TWIC to satisfy meeting the standard even without a reader. Submitting additional PII on individuals who have already been federally vetted and who also have a TWIC is burdensome to both DHS and industry and would be a wasteful and an ineffective use of agency and industry resources.

- **Providing 48 hours advance notification and submitting PII to DHS for personnel access:** While DHS has limited the 48 hour advance notice requirement to tier 1 and 2 sites, there is still a burden for those tier 1 and 2 sites to have to notify and submit PII to DHS with 48 hours advance notice of personnel accessing a facility. In addition to the burden, it is difficult to provide DHS with 48 hours advance notice for some instances involving contractors or emergencies. For example, if there is an emergency with equipment failures that need a quick turnaround to fix the problem or a change in subcontractors, then it may be necessary to provide access to those personnel without being able to provide DHS with 48 hours advance notice. However, those personnel may already be federally vetted with a TWIC so there really is no need to provide their PII since DHS already has that on record.

2. **How does the recent experience of the regulated community with the CFATS program compare with its experience at the time of the Subcommittee's last hearing on September 11, 2012? Are there improvements and, if so, what are they?**

Yes, AFPM acknowledges that there has been far greater outreach and much more detailed discussions by DHS with the regulated community this past year than previous years. However, it is still too early to tell the outcomes of that outreach since we haven't seen any final results yet. Specifically, AFPM is encouraged that DHS has conducted outreach meetings on how to improve the Topscreens, Site Vulnerability Assessments and Site Security Plans and created a peer review panel to review the site tiering methodology and modeling. These are two areas that AFPM had suggested that DHS re-engage industry two years ago.

3. What is the quality of communication between DHS and the regulated community? Is feedback systematic or based more on occasional, informal contacts?

DHS has had much better communication with stakeholders this past year than previous years. The method and the quality of the communication between DHS and the regulated community vary since it is sometimes informal and other times systematic. For example, the communication is systematic when DHS provides regular updates at trade meetings and at both the Oil & Gas and Chemical sector council meetings. However, there are other times when there will be an informal response from DHS, such as responding to emails, calls or telling information that would affect all industry to just one trade association.

However, the messages from DHS are still not coherent and reliable because there are still areas where the communication from DHS is inconsistent and should be improved. For example, the communications regarding the start-up of the clearance program has been disjointed at best. Considering the recent assessment by DHS of the cyber security threat, the clearance program start-up and process needs to be clearly communicated. To date that communication to industry stakeholders has largely been disjointed and inconsistent leaving the industry cyber security experts in clearance limbo. It is critical for cyber security of our nation's critical infrastructure that the process for this program gets communicated properly and clearly.

Another example is the use of certain terminology by DHS. For example, many in the regulated community, and we suspect Congress, are confused by how DHS interchangeably uses terms including "approved inspections" versus "authorized inspections" and "authorized plans" versus "conditional plans." Taken as a whole they are being used to show progress when that may not really be the case. AFPM recommends that DHS be clear and precise to Congress when using these terms.

4. Should feedback from the regulated facilities be more systematic through direct, detailed surveys? Would this significantly improve CFATS?

Given the backlog that DHS is experiencing with implementing the core CFATS program, AFPM does not think DHS will have the time or resources to review surveys. Instead of surveys, DHS should have the inspectors and protective security advisors continue their enhanced engagement with the sites. AFPM encourages DHS to continue with the pace of their recent outreach efforts which has significantly increased and improved over the past year. DHS should also be more systematic in their outreach to all stakeholders.

5. Overall, both DHS and GAO agree that there is progress on communication with the regulated community – do you think DHS has enabled you to fully understand the CFATS program and how DHS arrives at decisions?

AFPM is encouraged by the recent increased communication with the regulated community on many aspects of the CFATS program. However, greater transparency and informed discussions with the regulated community continue to be necessary to better understand how DHS arrives at decisions. This would lead to less confusion and quicken implementation for all parties. For example, AFPM recommends that DHS better communicate the reasons behind the decisions for site tiering.

AFPM is strongly concerned that the DHS risk modeling used for setting risk tier levels for facilities in CFATS is seriously flawed. AFPM continues to ask DHS to be more transparent regarding DHS risk modeling and risk tier level determinations. The risk modeling of the CFATS sites is the foundation of the CFATS program and AFPM is encouraged that DHS established a peer review panel to resolve the modeling issues. However, we again question why this was not done sooner as flaws in the risk modeling have been brought to DHS attention numerous times.

In the National Academies of Science's (NAS) 2010 "Review of the Department of Homeland Security's Approach to Risk Analysis," the NAS comments multiple times on the significance of stakeholder involvement and transparency in effective risk modeling. While NAS is commenting on risk assessment practices within DHS, the comment is directly applicable to CFATS implementation. The NAS recommendations for transparency and stakeholder input would benefit not only the risk assessment practices within the ISCD, but also provide substantial improvement on rule implementation.

The Honorable Henry A. Waxman

When the Committee drafted H.R. 2868 in the 111th Congress, several provisions were included to guide the tiering process for the CFATS facilities.

Section 2102 of the bill directed the Department of Homeland Security to first make a list of high risk facilities, based on a consideration of threat and consequence including adverse effects to human health, the environment, critical infrastructure, public health, homeland security, national security, and the national economy, as well as the geographic proximity to large population centers. Facilities on the list would then be sorted into tiers by the Department based on risk. Under this two step process, vulnerability would be considered in assessing risk and placing a facility into a tier, but not in determining whether a facility fell within the universe of CFATS regulated facilities. By removing vulnerability from the threshold determination of what facilities are covered by CFATS, this process might address the concern that a facility could cycle in and out of the regulated universe by adding or removing security measures.

1. **Do AFPM members support the consideration of vulnerability in determining the risk tier assignment for a facility, as set out in the National Infrastructure Protection Plan and the Interim Final Rule that created the CFATS program?**

Yes, vulnerability is an extremely important component in determining the risk tier assignment for a facility. The risk equation consists of three elements and all of them must be included when calculating risk, including consequence, vulnerability and threat. A facility that has implemented enhanced security measures is less vulnerable and therefore should be in a lower risk tier than a similarly situated facility that has not deployed enhanced security measures. Clearly, vulnerability is a factor in the risk equation and must be evaluated if DHS wants to accurately determine and sort tiers based on risk. If DHS ignores vulnerability and instead designates every site as having the same constant vulnerability, then DHS is ignoring the security systems and improvements that individual sites have implemented.

2. **Do AFPM members support the two step process set out in H.R. 2868, so that only threat and consequence would be considered in making the determination of whether a facility is subject to the CFATS regulations?**

No. For the reasons stated in question # 1, we cannot support a process that ignores facility vulnerability. Threat, consequence and vulnerability need to be considered when calculating the risk and determining whether a facility is subject to the CFATS regulations.

Section 2102 of the bill also outlined requirements for the Secretary of Homeland Security to provide owners and operators of covered facilities with the reason for the facilities tier assignment, and upon request, information related to the criticality of the facility, the proximity to other critical infrastructure, and the potential human consequences of a successful attack.

3. **Do AFPM members support requirements to provide that information to the owners and operators of covered facilities?**

Yes, AFPM members would support requirements for DHS to provide that type of information to the owners and operators of covered facilities because that would mean DHS would be transparent and provide details on the process. Some information provided upon request would be helpful to a facility's security risk mitigation efforts, such as the critical infrastructure near a site which may or may not be germane to the security of that site.

4. **Is there additional information that AFPM members would want to receive with their tier assignment to increase transparency and accountability in the tiering process?**

Yes, AFPM members would want to receive additional information that explains the methodology and framework for determining the risk tiering level. Currently, the process is not transparent and the methodology for the risk tiering process is not explained.

During the third panel of the hearing, you and other witnesses testified that under the existing CFATS framework, the regulatory process must be started over from the beginning any time a change is made in the facility. Section 2103 of H.R. 2868 called on the Secretary of Homeland Security to establish specific deadlines and requirements for the

submission of information describing material modifications to a covered facility's operation that may affect the security of a facility.

5. **Do AFPM members support increasing transparency and predictability in the CFATS regulatory process through the establishment of specific deadlines and requirements for the submission of information describing material modifications to facility operations?**

As the process is currently, if a site moves up or down a tier they would have to go through the whole CFATS process again and resubmit information to DHS. AFPM suggests that there is no tangible reason to do this unless there is a major change at a site that would affect their tiering level because it wastes resources of both industry and DHS. AFPM encourages DHS to re-engage industry on this issue as we believe a workable solution can be developed that would lessen the burden on both DHS and industry. AFPM submitted a proposal on how they might fix this issue to DHS in 2010 but has never received a response from DHS. In addition, if mandated, timeframes or deadlines need to be reasonable and not open to any outside litigation.

During the hearing, Timothy Scott of Dow Chemical testified that all Dow facilities regulated under the MTSA program are currently meeting security standards for tier 1 CFATS facilities, on a voluntary basis. H.R. 2868 would have ensured that all MTSA facilities were held to the appropriate risk-based standards to ensure an equivalent level of security for substances of concern at all facilities, while maintaining the Commandant of the Coast Guard as the primary regulatory authority for MTSA facilities.

6. **Are all AFPM members companies implementing security measures at MTSA facilities sufficient to meet the CFATS tier 1 standards?**

AFPM does not have member site information to support whether some facilities are or are not implementing security measures at MTSA facilities sufficient to meet the CFATS tier 1 standards. MTSA security measures are appropriate for those facilities that are regulated under the U.S. Coast Guard. AFPM does not support harmonization of the MTSA and CFATS programs and believes they should remain separate to avoid jurisdictional conflicts and duplication of efforts. However, AFPM recognizes that MTSA is an effective program and there are good lessons to be learned for implementing a truly risk-based program.

7. **Do AFPM members support requiring MTSA regulated facilities to meet security standards equivalent to the standards applicable to the tier such facilities would be assigned to if covered by the CFATS program?**

Currently the CFATS risk modeling tiering methodology is being peer reviewed so it is premature to even remotely consider having MTSA regulated facilities meet security standards equivalent to the standards applicable to the tier such facilities would be assigned to if covered by the CFATS program. MTSA security measures are appropriate for those facilities that are regulated under the U.S. Coast Guard. However, while MTSA is an effective program, it would be counterproductive to have MTSA facilities reassessed using CFATS methodology, particularly before some of the issues with the CFATS program have been addressed.

One frequently cited measure of success for the CFATS program is the number of facilities reducing their chemical holdings to no longer be deemed high risk.

8. How many facilities owned or operated by AFPM members have reduced their chemical holdings to "tier-out" of the CFATS program?

AFPM does not track our members tiering because specific site tiering is Chemical–terrorism Vulnerability Information (CVI). In general, we are aware that some of our member sites have tiered down or tiered out by using a variety of methods. AFPM doesn't keep individual member data because it is CVI. AFPM supports the ability to tier-down or tier-out a facility based upon changes made on-site; however, each facility is unique and the ability to reduce chemical holdings or deploy specific security risk mitigation measures varies from site-to-site.

9. What chemicals, processes, or technologies, have those facilities used to reduce their holdings of substances of concern?

See above response to question #8. AFPM members have used a variety of ways to reduce their holdings of substances of concern including but not limited to just in time delivery, volume reduction, shifting storage, and managing inventory. AFPM strongly notes however that each facility is unique and the ability to reduce chemical holdings or deploy specific security risk mitigation measures varies from site-to-site with many factors that must be considered.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

April 4, 2013

Mr. Rick Hind
Legislative Director
Greenpeace
702 H Street, N.W.
Washington, D.C. 20001

Dear Mr. Hind:

Thank you for appearing before the Subcommittee on Energy and Power on Thursday, March 14, 2013, to testify at the hearing entitled "The Chemical Facility Anti-Terrorism Standards Program – A Progress Update."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Thursday, April 18, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Nick.Abraham@mail.house.gov and mailed to Nick Abraham, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

John Shimkus
Chairman
Subcommittee on Environment and the Economy

cc: The Honorable Paul Tonko, Ranking Member,
Subcommittee on Environment and the Economy

Attachment

The Honorable Henry A. Waxman

The Department of Homeland Security's outreach to facility owners and operators as well as stakeholders, including state and local governments and trade associations was one focus of the Government Accountability Office's testimony for this hearing, but outreach to other stakeholders was not described.

1. What communication and outreach have you and other members of the Blue Green Alliance received over the course of the CFATS program?

NOTE: The Coalition to Prevent Chemical Disasters is made up of more than 100 organizations including major unions, public health, national security, 9/11 widows, environmental justice and national green groups. The Blue Green Alliance, like Greenpeace is one of many participating organizations in this coalition.

The April 17, 2013 disaster in West, Texas is a grim reminder of the catastrophic hazards posed by facilities that use and store ultra hazardous substances. http://www.nytimes.com/2013/04/19/us/huge-blast-at-texas-fertilizer-plant.html?_r=0 Tragically we have yet to set safety standards that will prevent these disasters or dramatically reduce their lethality by switching to safer processes. There are more than 470 chemical facilities in the U.S. that each put 100,000 or more people at risk of serious injury or death. Given these continuing hazards and the availability of safer more secure processes the only responsible public policy is to adopt safety standards that protect workers and communities when industrial systems fail, hurricanes strike or terrorist attack.

Members of our coalition have continually reached out to the DHS throughout the course of the CFATS program. We have requested meetings, submitted comments and a requested greater access to the DHS in the development and implementation of the CFATS program.

Greenpeace and other organizations and members of Congress submitted formal comments criticizing the DHS's proposed interim CFATS rules. For example, Greenpeace's May 17, 2007 comments are at:
https://www.documentcloud.org/documents/684443-gpcommentsondhsproposedregs.html
Our coalition submitted comments on CFATS Risk Based Performance Standards onNovember 25, 2008:
https://www.documentcloud.org/documents/684440-chemseccoalitioncomments-to-dhs-rbps-nov-2008.html

Labor has also had conversations with DHS about background checks as part of the personnel surety portion of CFATS on Oct 15, 2012. This included the ICWUC, USW, Teamsters, CWA and UAW. Labor, a crucial stakeholder, has only been marginally involved by DHS over the course of the CFATS program while industry has had enormous influence, in some cases, at the expense of workers' rights.

In addition in an August 24, 2010 letter to the DHS Greenpeace raised concerns about excessive secrecy and conflicts of interest regarding the non-FACA advisory group made up of chemical industry trade associations and chemical companies known as the Chemical Sector Critical Infrastructure Partnership Advisory Council (CIPAC). Although CIPAC is paid for by the federal government, it operates autonomously and provides

regular access and opportunities for inappropriate influence by the regulated industry over its regulator both in the development of rules and their implementation. For more details, see the November 25, 2010 Washington Post story on CIPAC: http://www.washingtonpost.com/wp-dyn/content/article/2010/11/24/AR2010112407022.html

Greenpeace sent the DHS a complaint about CIPAC on August 24, 2010 http://research.greenpeaceusa.org/index.php?a=view&d=4849;
On November 2, 2010 the DHS defended CIPAC but agreed to meet with our coalition twice a year.http://research.greenpeaceusa.org/index.php?a=view&d=4847
In our November 4, 2010 response we urged them to dissolve the CIPAC and run it under the rules of the Federal Advisory Committee Act: http://research.greenpeaceusa.org/index.php?a=view&d=4846

Since that time representatives of our coalition have met in person or by conference call with DHS staff approximately twice a year.

The GAO and officials at the Department have reported on the development of a new strategic communication plan for the CFATS program.

2. Have you or other members of the Blue Green Alliance been consulted in the development of this strategic communication plan?

We are unaware of any coalition partners who have been consulted by the DHS on their strategic communications plan.

3. Please provide a list of public interest stakeholders that you believe should be included in communication efforts under the strategic communication plan.

All members of our coalition should be included, most of which are listed on the June 21, 2011 letter to the U.S. House of Representatives from more than 100 organizations: http://research.greenpeaceusa.org/index.php?a=view&d=6001

When the Committee drafted H.R. 2868 in the 111th Congress, several provisions were included to guide the tiering process for CFATS facilities and provide greater transparency. That bill also would have closed significant security gaps, so that a higher proportion of holdings of substances of concern would be secured.

4. Based on your analysis of publicly available information on holdings of substances of concern, are you satisfied that the CFATS program is covering a high proportion of those holdings?

No. There is no publicly available accountability information on which facilities are in the CFATS program or even which facilities have adopted safer processes and are no longer in the CFATS program. The DHS has provided aggregate data which confirms that potentially thousands of high risk facilities continue to be exempt from CFATS. For example, in the testimony from Undersecretary Rand Beers dated March 14, 2013 he stated: "As of March 5, 2013, CFATS covers 4,380 high-risk facilities nationwide." Compared to the 12,440 facilities reported in the Nov 6, 2012 survey by Congressional Research Service of the EPA's risk management program this does not constitute a "high proportion" of these holdings. This data also shows that very few facilities that pose a catastrophic "release" risk remain in the CFATS program. For example there are only

35 "release" category facilities in risk tiers 1 and 2. Meanwhile there are 473 facilities in the EPA's RMP program that each pose a hazard to 100,000 or more people. If CFATS were a comprehensive program it would cover these facilities.

Some of the highest risk facilities in the country are instead nominally regulated by a patchwork quilt of statutes such as the Maritime Transportation Security Act (MTSA), Clean Water Act and Safe Drinking Water Act (an estimated 2,400 water facilities). None of these statutes require risk reduction or prevention measures to be taken. In fact, the MTSA has historically been the industry model for "alternative security programs" (ASPs). Exempt facilities include the infamous Kuehne Chemical plant in South Kearny, NJ which puts 12 million people at risk and the largest chemical facility in the nation, Dow Chemical's Freeport, Texas facility and a majority of U.S. refineries.

On April 16, 2013 the United Steelworkers (USW) released a new report, "A Risk Too Great" that lists 50 refineries that together put more than 26 million people at risk. Do the communities adjacent to these plants or their members of Congress know which security standards each these facilities are held to? The USW report is at:http://assets.usw.org/resources/hse/pdf/A-Risk-Too-Great.pdf

By contrast the EPA's RMP program has seen a net increase in high risk facilities over the last two years. A November 16, 2012 Congressional Research Service (CRS) update of the number of highrisk chemical facilities in the EPA's chemical disaster or Risk Management Program (RMP) shows a growing number of chemical facilities that each put thousands of people at risk of a catastrophic chemical release.https://www.documentcloud.org/documents/557127-crs-rmp-update-11-16-12.html

In 2012, there were 12,440 EPA facilities nationwide that possessed thresholds quantities of ultra-hazardous chemicals requiring reports to the EPA of their "worst case" disaster scenarios. This was an increase of 79 facilities over the CRS's 2011 update on this EPA program. https://www.documentcloud.org/documents/557129-crs-update-of-us-rmps-state-by-state-4-12-11.html

The increase in 2012 included 28 additional facilities that put between 10,000 and 99,999 people at risk in the following states: Arizona, California, Colorado, Kansas, Louisiana, New Jersey, New Mexico, New York, Ohio, Oregon, Rhode Island, South Dakota, Texas, Utah, and Washington.

The 2011 CRS update showed an increase of 332 in the total number of RMP facilities over the 2009 CRS update. https://www.documentcloud.org/documents/557128-crs-update-2009.html

5. Are you satisfied that tiering under the program has been accurate to date?

The criteria for tiering is too secretive to provide credible public accountability as to whether facilities are put in the correct tier. Moreover if the program continues to focus on risk management over risk reduction or prevention it will continue to ignore the most fool proof security measures available, safer and more secure chemical processes. The current tiering also apparently does not account for the shifting of hazards onto inherently vulnerable modes of transportation, in particular the use of rail cars to ship Toxic Inhalation Hazard substances. This could in part be improved by issuing new performance standards or new legislation. In the absence of new performance

standards or legislation we recommend that the EPA use it's authority under the Clean Air Act to issue new risk reduction or prevention rules and guidance as the Agency proposed following the 9/11 attacks in 2002.

6. Do you and other members of the Blue Green Alliance still support provisions in H.R. 2868 to close security gaps, guide tiering, and increase transparency?

Yes, our June 21, 2011coalition letter to the U.S. House of Representatives from more than 100 organizations restates support for those fundamental improvements to chemical security policies at: http://research.greenpeaceusa.org/index.php?a=view&d=6001

H.R. 2868 also would have required all facilities to assess methods to reduce the consequences of a terrorist attack, and would have required the highest risk facilities to implement those methods where feasible. The Department of Homeland Security continues to support that approach.

7. Do you and other members of the Blue Green Alliance continue to support requirements for assessments and where feasible implementation, of methods to reduce consequences of a successful attack?

Yes, our June 21, 2011 coalition letter to the U.S. House of Representatives from more than 100 organizations restated our support for that policy at: http://research.greenpeaceusa.org/index.php?a=view&d=6001

It was also recently included in an April 16, 2013 report by the United Steelworkers, "A Risk Too Great" at: http://assets.usw.org/resources/hse/pdf/A-Risk-Too-Great.pdf

8. Do you and other members of the Blue Green Alliance support consistent requirements for consideration and adoption of methods to reduce the consequences of an attack across sectors, including water facilities, government owned or operated facilities, and facilities regulated under MTSA?

Yes, this is also restated in our June 21, 2011 coalition letter to the U.S. House of Representatives from more than 100 organizations at: http://research.greenpeaceusa.org/index.php?a=view&d=6001

The coalition and member unions such as the United Steelworkers strongly support requirements for inclusion of facilities currently not included in CFATS. Many of union members work in public sector water treatment facilities and at oil refineries or chemical plants that are located on waterways and are therefore covered under MTSA. These facilities are no less vulnerable to a release or attack than facilities covered by CFATS.

An example of this was the April 16, 2013 report by the United Steelworkers, "A Risk Too Great" about refineries that together put more than 26 million people at risk while safer processes go unutilized:http://assets.usw.org/resources/hse/pdf/A-Risk-Too-Great.pdf

One frequently cited measure of success for the CFATS program is the number of facilities reducing their chemical holdings to no longer be deemed high risk.

9. What efforts have you undertaken to gather information about the data behind this measure of success, e.g. types of facilities making this change, as well as

chemicals, processes, and technologies used to reduce the facilities holdings of substances of concern?

The Center for American Progress (CAP) has done several reports analyzing EPA's Risk Management Program data. The first in 2006 identified 284 facilities that have converted from the use of large amounts of acutely hazardous substances since 1999. See full report at: http://www.americanprogress.org/issues/2006/04/b681085_ct2556757.html

A 2010 CAP project identified 554 water and wastewater treatment facilities that had converted to a safer and more secure alternative. These facilities are identified at: http://www.americanprogress.org/issues/security/news/2010/03/02/7539/safer-chemicals-create-a-more-secure-america/

While the CAP reports provide concrete examples of the availability and feasibility of safer alternatives, most of the examples of converted facilities are not at the highest risk facilities, indicating that many of the highest hazard facilities are not converting under the current CFATS program. Nonetheless, a CAP report, Chemical Security 101, identified facilities in many of the highest hazard industries that already conduct operations without posing the danger of a major toxic gas release. The CAP also produced a fact sheet that listed intrinsically more secure options:
"Intrinsically More Secure: Alternatives for Many Industries
• Bleach manufacturers eliminate bulk chlorine gas by generating chlorine as needed "just in time" on-site, eliminating transportation and storage vulnerabilities.
• Petroleum refineries avoid dangerous hydrofluoric acid alkylation by using less hazardous sulfuric acid; others are developing solid acid catalysts.
• Water utilities eliminate bulk chlorine gas by using liquid bleach, ozone without storage, and ultraviolet light as appropriate.
• Paper mills eliminate bulk chlorine gas by using hydrogen peroxide, ozone, or chlorine dioxide without bulk storage.
• Pool service companies eliminate chlorine gas by using chlorine tabs or liquid bleach.
• Manufacturers of polyurethane foams eliminate bulk ethylene oxide by substituting vegetable-based polyols.
• Soap and detergent manufacturers eliminate bulk oleum and sulfur trioxide by using sulfur burning equipment on-site.
• Manufacturers of ferric chloride eliminate bulk chlorine gas by processing scrap steel with less concentrated liquid hydrochloric acid (less than 37 percent) and oxygen.
• Titanium dioxide producers eliminate bulk chlorine gas by generating chlorine on-site as needed without storage, or by using the sulfate process.
• Secondary aluminum smelters eliminate bulk chlorine gas by removing impurities with nitrogen gas injected with magnesium salts.
• Manufacturers of semiconductors, silicon wafers, and metal products eliminate concentrated hydrofluoric acid by using less concentrated forms (less than 50 percent).
• Power plants eliminate bulk anhydrous ammonia gas by using cleaner combustion or by using aqueous ammonia or urea in pollution control equipment; they also remove chlorine gas by using liquid bleach to treat cooling water.
• Wholesale chemical distributors eliminate most bulk chlorine gas and sulfur dioxide gas by distributing alternatives such as liquid bleach and sodium bisulfite.
• Pulp mills, food processors, wastewater plants, and hazardous waste recovery operations eliminate bulk sulfur dioxide gas by, as appropriate, generating sulfur compounds on-site or purchasing sodium bisulfite, metabisulfite, hydrosulfite, or other alternatives.
• Diverse manufacturers eliminate bulk chlorine gas by generating chlorine on-site as needed without storage, such as for fuel additives, water treatment chemicals, and aramid polymers used to make bulletproof vests."

The April 16, 2013 USW report, "A Risk Too Great" also suggests that refineries currently using hydrofluoric acid (HF) switch to safer more secure alkylation processes: http://assets.usw.org/resources/hse/pdf/A-Risk-Too-Great.pdf

Unlike the data available at the EPA's reading rooms, the DHS has refused to make public the facilities that no longer are in the CFATS program due to a change in their use of regulated chemicals. After requesting this information from the DHS numerous times over the past few years, on May 18, 2012 Greenpeace asked for this information in a Freedom of Information Act request: https://www.documentcloud.org/documents/684442-foia-to-dhs-5-18-12.html
That FOIA request was denied on March 13, 2013:
https://www.documentcloud.org/documents/684441-dhs-foia-interim-response-letter.html

10. What have you been able to find out about the data behind this measure of success?

We believe that the federal government lacks systematically gathered information about methods that are available to reduce the consequences of a chemical disaster at a chemical facility. The federal role would be immeasurably strengthened and made more knowledgeable by requiring tiered facilities under CFATS to assess and report to DHS on methods to reduce the consequences of a terrorist attack. We also strongly support requiring facilities covered by the Risk Management Planning requirements of the Clean Air Act assess and report to EPA on methods that reduce the consequences of an accidental release. Lack of familiarity with safer and more secure chemical process is a major hindrance to an effective federal response to chemical safety and security issues.

We have repeatedly asked the DHS for specific examples of facilities that have "tiered out" of CFATS by changing their processes or eliminating the use of ultra-hazardous chemicals of interest (COI) regulated under CFATS. On May 18, 2012 we requested this information under the Freedom of Information Act (FOIA):https://www.documentcloud.org/documents/684442-foia-to-dhs-5-18-12.html
That FOIA request was denied on March 13, 2013:
https://www.documentcloud.org/documents/684441-dhs-foia-interim-response-letter.html

Withholding this information is not in the public interest. If these facilities are no longer attractive targets they could be a model for other facilities to also become unattractive targets.

In 2011 USW members at a facility alerted the union's Health, Safety & Environment Department that the company they worked for was parking multiple rail tankers containing highly hazardous chemicals outside the plant's fence line. The risk of an accidental or criminal action causing a release was even more likely for these rail cars that sat unguarded. The experience of finding a government agency to hold the company accountable was alarming. No agency, including DHS under CFATS, would say that it was within their jurisdiction. The chemicals were outside the fence and therefore not necessarily required to be reported although they certainly posed a risk. Due to a labor dispute at the facility, we do not know the precise reason for parking them outside the fence; but this is an example of risk shifting. While there is no way to gauge how common risk shifting is at CFATS-covered facilities, it remains a concern when facilities report reducing their holdings of substances of concern without disclosing how that was done.

During the hearing, ISCD Director David Wulf testified that feedback from facility operators regarding inspections was "favorable" and "positive." Industry witnesses also testified that the inspection experience under the CFATS program has been congenial. One witness even testified that "Inspectors are providing sufficient details with facilities prior to their arrival, which aids the planning process to ensure resources and facility personnel are available." Section 550 does not require unannounced "inspections, and they are not currently conducted.

11. Are unannounced inspections important to ensuring compliance with the CFATS standards?

Unannounced inspections are critical to ensuring compliance and are commonplace in government safety regulations. We see unannounced inspections by OSHA, MSHA and in other areas of safety regulations including food and fire safety. Good actors have nothing to fear from unannounced inspections, and bad actors don't have time to hide noncompliance when they don't receive advanced notice. Another critical aspect of productive inspections is involving the union or a designated worker representative at facilities. These workers truly know what is happening on-the-ground in the facility and would be a valuable resource during CFATS inspections. At this time CFATS inspections do not include union or worker representation.

Unannounced inspections were contained in H.R. 2868 as a common sense component of enforcement and accountability.

Many of the problems now identified in the CFATS program were brought to light when an anonymous whistleblower leaked the internal November 2011 memorandum. Without that whistleblower action, many of the deficiencies might still be hidden from view.

12. In your view, how important are whistleblower protections to ensure that policy makers and the public are aware of issues in the implementation of the CFATS program?

Strong whistleblower protections are very important not only for DHS implementation of the program, but also at CFATS-covered facilities where workers or others may need to blow the whistle on a company failing to comply or properly implement CFATS. Whistleblower protections are particularly important due to part of the personnel surety portion of CFATS. The program allows companies to do background checks that are far beyond identification, immigration status, criminal background and the terrorist database. Under CFATS companies can unnecessarily look into high school transcripts, credit reports, misdemeanor records, and other irrelevant documents that can be used to intimidate workers who want to speak out. Whistleblowers need to know that they will be protected.

In addition, comprehensive chemical security legislation should include regular public reports to Congress on the progress of the program (including the use of background checks). Such provisions were included in H.R. 2868 as passed the House in 2009. These reports would have brought to light many of the current deficiencies in CFATS in a time manner, had they been enacted.

○