U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Environment and Climate Change

Hearing Entitled: "Protecting and Securing Chemical Facilities from Terrorist Attacks"

Written Testimony by Scott Whelchel on behalf of the American Chemistry Council

Wednesday, September 11, 2019

10:00 am in the John D. Dingell Room, 2123 Rayburn House Office Building

Introduction

Scott Whelchel is the Chief Security Officer and Global Director of Emergency Services and Security for Dow, the leading multi-national manufacturer of chemical products. Dow operates 113 manufacturing sites in 31 countries and employs approximately 37,000 people. The Company's portfolio of performance materials, industrial intermediates, and plastics businesses that delivers a broad range of differentiated science-based products and solutions for our customers in high-growth segments, such as packaging, infrastructure, and consumer care.

Scott is also the Vice Chair of the Chemical Sector Coordinating Council and is a distinguished member of the Security Committee of the American Chemistry Council (ACC).

Prior to joining Dow, Scott was the Director for St. Charles Parish Department of Homeland Security and Emergency Preparedness and is Past-President of the Louisiana Emergency Preparedness Association. Scott worked in the U.S. Intelligence Community for over 24 years in both a military and civilian service capacity. During his intelligence career, he served as a Senior Intelligence Officer for the Office of the Director of National Intelligence and Counterintelligence Officer for the Department of Defense in the Federal Civilian Service in Washington, DC.

The business of chemistry is a $553 billion enterprise; providing more than 540,000 skilled, good-paying American jobs. The average annual salary of a U.S. chemical industry employee is $86,000, which is 25 percent higher than the average U.S. manufacturing pay. The chemical manufacturing industry is experiencing a renaissance in the United States thanks to the increase in domestic shale gas production. In fact, the ACC has identified more than 330 new capital investment projects worth more than $200 billion adding tens of thousands of jobs and generating almost $300 billion dollars in economic activity.

ACC represents a majority of the chemical producers across the United States, including a diverse set of small and medium-sized companies engaged in the business of chemistry. ACC member companies manufacture products that are critical to the everyday health and well-being of our nation and are essential to developing a more sustainable and more competitive economy. For this reason - but primarily due to our responsibility to protect our employees and the communities in which we operate - chemical security is a top priority for Dow and for all ACC member companies.

Responsible Care® Security Code

In 2001, the ACC created the Responsible Care® Security Code, a stringent, mandatory security program for ACC member companies. Since it was established, ACC member companies have invested more than $23 billion to further enhance their site security, transportation security, and cybersecurity. The Security Code is the gold standard for the industry and serves as a model for regulatory programs around the world.

The Need to Reauthorize CFATS with Program Improvements

ACC supports a long-term reauthorization of the Chemical Facility Anti-Terrorism Standards (CFATS) program. Ensuring that the CFATS program remains in place is a crucial part of establishing a stable regulatory environment, and providing the needed certainty to foster long-term security investments.

Program Improvements

Since 2014, the Department of Homeland Security (DHS) has significantly improved its administration of the CFATS program, which has had a significant impact on enhancing chemical security across the United States. Several factors have led to its recent success, including:

- Improved site security inspectors and inspections;
- Improved risk assessment process;
- Improved Site Security Plan (SSP) authorization process; and
- A commitment to work with the regulated community to improve the program.

While DHS has made considerable strides to enhance the CFATS program, ACC offers the following recommendations to further improve the program.

- Ensure Long-Term Multi-Year Authorization.

Recently, Congress approved a short-term (15 months) extension to the CFATS program, following a previous 4-year authorization period. Longer authorization periods provide important stability for covered facilities to effectively plan for security investments, as well as enabling DHS to efficiently manage the program.

Periodic Congressional oversight of the program is important for assessing the efficacy of the CFATS program in meeting a changing security environment. Therefore, a long-term reauthorization of the CFATS program is necessary to meet these key objectives: oversight, stability and efficiency.

- Assess the value of Terrorist Screening Database (TSDB) vetting at lower risk facilities.

DHS recently began implementing phase one of Risk Based Performance Standard 12(iv), screening individuals for terrorist ties. Phase one was limited to approximately 240 of the highest risk CFATS facilities in Tiers 1 and 2. This process requires CFATS facilities to collect

sensitive personal identifying information (PII) from thousands of employees and contractors and transmit that information over the internet to DHS for vetting against the TSDB.

DHS has begun to significantly expand this requirement to more than 3,000 lower risk facilities, Tiers 3 and 4. This would include the personal information of an additional tens of thousands of employees and contractors. ACC believes that such an expansion is unnecessary and will needlessly create a security risk by exposing thousands of individual records to loss or cyber theft and operational interruptions (false positives, etc.). Further, we believe the benefit with TSDB vetting at lower risk facilities is minimal at best. While we support TSDB vetting at the highest risk Tier 1 and Tier 2 facilities, we strongly recommend that Congress reconsider this requirement for the lower risk, Tier 3 and Tier 4 facilities.

- Improve transparency in DHS CFATS risk determinations.

DHS needs to be more transparent with CFATS facilities regarding the specific factors driving risk at their location. Furthermore, DHS should proactively engage CFATS facilities to reduce risk. Often, covered facilities are not fully aware of the specific threat driving CFATS risk at a specified tier level. It is the site security manager who has the overall responsibility and authority for making critical security risk management decisions at CFATS facilities and the facility security director should be fully informed by DHS of all details related to threat and risk. If needed this can be done in a classified setting.

- Establish a CFATS Recognition Program

DHS should leverage Industry Stewardship Programs, such as ACC's Responsible Care, by establishing a Regulatory Recognition Program under CFATS. By doing so, DHS would recognize responsible operators for going above and beyond mere regulatory compliance and incentivize the creation of new stewardship programs.

Performance data show facilities that participate in well-established stewardship programs out perform their peers and the industry overall. By providing regulatory incentives, DHS can influence improved performance beyond the universe of the CFATS-regulated community and prioritize their efforts where they are most needed.

- Maintain a Security Program Focus

It is also important for the CFATS program to maintain its security focus. The program's continued success will depend upon its ability to help manage security risks. The CFATS program should not stray beyond its primary function of addressing security risks and into areas already addressed by well-established environmental, health and safety regulatory programs administered by other federal and state agencies. Adding additional safety and labor requirements could impair the CFATS program focus on security risk, and will impede its progress towards the goal of protecting critical infrastructure.

- Information Sharing and Coordination

Protecting our people, communities and operations from security risk is never taken lightly. We engage and include all necessary experts and stakeholders to ensure security plans are solid, comprehensive and sustainable. Coordination activities with local emergency planners, first responders and law enforcement are essential to effectively responding during an incident at any facility, especially at those which are designated as high risk.

Reauthorization legislation should not permit the disclosure of site security information to the public, or anyone who does not have a need to know to obtain such information. Facilities must protect sensitive information from individuals that might pose a threat to employees, property or surrounding communities. Sensitive information—such as security system designs, control system schematics, worst case scenario discharge data, Chemical of Interest (COI) records, Chemical-terrorism Vulnerability Information, and tactical response information for emergency personnel—could threaten security if it falls into the wrong hands.

The current regulatory framework strikes the right balance to ensure that those with a need-to-know have the information they need to respond effectively. Risk Based Performance Standard (RBPS) 9 requires CFATS facilities to develop a response plan and coordinate with local response groups. CFATS compliance inspectors will not approve a facility's Site Security Plan (SSP) if this coordination has not happened.

- Cybersecurity

Cybersecurity is an important element of a comprehensive security risk management system. Cyber requirements and needs vary greatly across the chemical sector. The CFATS program includes Risk Based Performance Standard (RBPS) 8, which is a performance standard that addresses the deterrence of cyber sabotage including the prevention of unauthorized on-site or remote access to critical process controls and critical business systems, and other sensitive computerized systems. The level and degree of cyber protections expected at facilities increases in correlation to their level of cyber integration.

For example, at Dow, they are implementing a manufacturing cybersecurity strategy to complement their enterprise strategy. This includes the placement of cybersecurity specialists inside their facilities to provide tailored security to the manufacturing assets needing additional layers of protection.

ACC believes that DHS could do a better job in sharing cyber threat information with CFATS facilities. This type of data would be very helpful for facilities to prioritize their risk evaluation and security planning. DHS inspectors should also be trained in the latest cybersecurity threats, techniques and incidents against chemical operators and handlers so it can be shared with regulated facilities and plans adapted accordingly.

- Voluntary Programs and Outreach

Since its inception, the DHS infrastructure protection program has developed a wealth of valuable tools and voluntary programs which have made a considerable difference in reducing the risk of hazardous chemicals. These tools and outreach activities should be expanded and

made available to the broader chemical community including non CFATS regulated facilities. DHS should embrace a comprehensive strategy to effectuate meaningful chemical risk reduction including regulation, voluntary programs and recognition of industry programs.

Conclusion

The CFATS Program has made our industry, our communities and our country more secure. CFATS will grow stronger by adopting the improvements outlined in this testimony and through the continued engagement of this Committee to ensure the CFATS program stays on track.

The long-term security of our nation is a goal and a commitment that we all share. ACC and its member companies encourage you to provide the much-needed stability to this important security program through a long-term reauthorization, and make the necessary improvements to the program while providing DHS with the appropriate Congressional oversight and guidance.