US House of Representatives, Subcommittee on Cybersecurity, Infrastructure Protection and Innovation

Hearing Entitled: "Securing our Nation's Chemical Facilities: Stakeholder Perspectives on Improving the CFATS Program"

Testimony by Kirsten Meskill on behalf of Kirsten-Meskill-Testimony-on-Securing-our-Nations-Chemical-Facilities-031219 the American Chemistry Council

Tuesday, March 12, 2019

10:00 am in 310 Cannon House Office Building

Thank you, Chairman Richmond, Ranking Member Katko and members of the Subcommittee for inviting me to participate in today's hearing. I am the Director of Corporate Security for the BASF Corporation. Headquartered in Florham Park, New Jersey, BASF operates over 100 production facilities with a footprint in 30 states and employs more than 20,000 people across North America. BASF's largest sites are located in Geismar, Louisiana and Freeport, Texas.

I have also served as the Chair of the Chemical Sector Coordinating Council and I am current Chair of the Security Committee of the American Chemistry Council (ACC), on whose behalf I am testifying today. 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.

The business of chemistry is a $526 billion enterprise; providing more than 500,000 skilled, good-paying American jobs. The chemical manufacturing industry is experiencing a renaissance in the United States thanks to the increase in domestic shale gas production. In fact, 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.

BASF has a responsibility to protect our employees and the communities in which we operate, so chemical security remains a top priority for us and for all member companies of ACC. In fact, in 2001, ACC created a stringent, mandatory security program known as the Responsible Care® Security Code. Since the Security Code was established, ACC members have invested more than $17 billion to further enhance site security, transportation security and cybersecurity at all member facilities. The Security Code has become the gold standard for the industry and serves as a model for regulatory programs.

ACC supports a long-term reauthorization of the Chemical Facility Anti-Terrorism Standards (CFATS) program. Ensuring that CFATS 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

Over the past few years, the Department of Homeland Security (DHS) has significantly improved its administration of the CFATS program; having a positive impact on chemical security across the United States. Several factors have led to its recent success, including: Improved site security inspections; improved risk assessment; and, a more streamlined and consistent Site Security Plan (SSP) authorization process. Most importantly, DHS leadership has demonstrated a willingness and commitment to work with the regulated community to help improve the program.

While DHS has made considerable strides to enhance the CFATS program, more work needs to be done. ACC would like to offer the following recommendations for CFATS improvement:

1. Ensure 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 planning security investments, as well as allowing DHS to efficiently manage the program. Periodic Congressional oversight of the program is also important for assessing the efficacy of CFATS to meet a changing security environment. Therefore, a multi-year reauthorization of the CFATS program is necessary to meet these key objectives: oversight, stability and efficiency.

2. Assess the value of TSDB Screening at lower risk facilities.
   Over the past couple years, DHS has been 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 information from thousands of employees and contractors and transmit that information over the Internet to DHS for vetting against the Terrorist Screening Database (TSDB).

   DHS is planning to significantly expand this requirement to more than 3,000 lower risk facilities, Tiers 3 and 4, involving tens of thousands of employees and contractors' personal information. ACC believes 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 (e.g., false positives, etc.). Further, the benefit associated with TSDB vetting at these lower risk facilities is minimal at best. While we support TSDB vetting at highest risk Tier 1 and Tier 2 facilities, we strongly recommend DHS reconsider this requirement for the lower risk, Tier 3 and Tier 4 facilities.

3. Improve transparency in DHS risk determinations.
   DHS should be more transparent with CFATS facilities regarding the specific factors driving risk at each location. Further, DHS should proactively engage CFATS facilities to reduce risk. CFATS facilities are not fully aware of the specific threat driving risk at a specified tier level. Site managers have the overall responsibility and authority for making critical security risk management decisions at CFATS facilities and are directly responsible for protecting the site

and its operations. The facility manager or responsible 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.

4. Establish a CFATS Recognition Program.
   DHS should leverage Industry Stewardship Programs, such as ACC's Responsible Care Security Code, by creating a Recognition Program under CFATS. By doing so, DHS would be able to recognize responsible operators for going beyond regulatory compliance and incentivize the creation of new stewardship programs. Performance data shows that facilities that participate in well-established stewardship programs perform better than their peers who do not, and better than the industry overall. By providing regulatory incentives, DHS can expand improved performance beyond the universe of the CFATS regulated community and prioritize their efforts where they are needed the most. This would also help to lessen the burden of security regulation on industry partners that balance similar yet disparate requirements of other security regulations under USCG, DEA, TSA, FDA, etc.

CFATS has helped make our industry and communities more secure. It is a program that will grow stronger by adopting the improvements outlined above and by the continued engagement of this committee to make sure CFATS stays on track.

Maintain Program Focus

It is also important that CFATS maintain its security focus. The continued success of the CFATS program will depend upon its ability to help manage security risks. CFATS should not stray into areas outside of its primary function of addressing security risks and into areas already addressed by well-established environmental and safety regulatory programs administered by other federal and state agencies. Layering on additional responsibilities could impair its focus and will impede its progress toward the goal of protecting important critical infrastructure from security threats.

Information Sharing and Coordination

Coordinating with local emergency planners, first responders and law enforcement is essential to ensure an effective response during an incident at any facility, but especially at high-risk ones. In fact, it is in the facility's best interest to make sure this happens in order to protect its employees, local communities and continuity of operations. It is equally important that the sharing of sensitive information is done on a need-to-know basis.

The current regulatory framework strikes the right balance to ensure that those with a need-to-know have sufficient information to respond effectively. Risk Based Performance Standard (RBPS) 11 requires CFATS facilities to coordinate emergency plans with local response groups. CFATS compliance inspectors will not approve a facility's Site Security Plan (SSP) if this coordination has not occurred.

Protecting our people, communities and operations from security risk is never taken lightly. We engage and include all the necessary experts and stakeholders to ensure our security plans are solid, comprehensive and sustainable. If any issues arise, they can be addressed collaboratively. CFATS covers these important areas to help ensure that regulated facilities are taking a sound approach to developing security plans and providing opportunities for feedback.

Cybersecurity

Cybersecurity is an important element of a comprehensive security risk management system. Cyber requirements and needs vary greatly across a diverse chemical sector. CFATS 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 protection expected at facilities increases in correlation to its level of cyber integration. ACC believes that DHS could do a better job in sharing cyber threat information with CFATS facilities. This data would be very helpful for facilities to prioritize risk evaluation and security planning. DHS inspectors should also be trained in the latest trends in cybersecurity threats against chemical operators and handlers so those trends can be shared with regulated facilities and plans can be adapted accordingly.

Conclusion

The long-term security of our nation is a goal and a commitment that we all share. That is why ACC and its members encourage you to provide the necessary stability to this important security program and make the improvements that are needed to take CFATS to the next level while providing DHS with the appropriate Congressional oversight and guidance.