Subcommittee on Environment and Climate Change
Hearing on
"Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2019"
September 11, 2019

Mr. Scott Whelchel
Chief Security Office and Global Director of Emergency Services and Security
Dow

The Honorable John Shimkus (R-IL)

1. How are facilities coordinating with or otherwise sharing information with emergency responders and state and local government officials?

RESPONSE: *Dow, like all ACC members, have an established Community Outreach Program focused on protecting the environment, health, and safety of the community and increasing confidence in the safe use of chemical technology through:*

- *Communicating clearly and transparently*
- *Engaging in conversations*
- *Collaborating*
- *Conducting research*

Stakeholders include, but are not limited to:

- *Employees on site*
- *Residents & community representatives*
- *Local & state authorities*
- *Law enforcement agencies*
- *Local emergency planning organizations (LEPCs)*
- *Community Advisory Panels (CAPs)*
- *Educational institutions*
- *Media*
- *Customers*
- *Suppliers*
- *Tenants*

Each Dow location must have a documented Community Outreach Program through which it can share details on:

  - *Site operations*
  - *Products, applications & innovation*
  - *Product distribution*
  - *Corporate Social Responsibility*
  - *Projects to protect the community's safety, health, and environment*

Maintain dialog with stakeholders regarding:

- *Emergency Response Plans (internal & external)*
  - *Preparedness plans*
  - *Distribution emergency response*
  - *Emergency drills*
- *Chemical inventories*
- *Reduction of waste and emissions*
- *Reduction of water and energy consumption*
- *Process safety systems*
- *Questions, concerns and expectations*
- *Opportunities to educate and improve community confidence*

a. Should persons getting access to Chemical Vulnerability Information (CVI) have both a need to know and be trained in handling CVI?

RESPONSE: *Yes*

b. In addition to CFATS, are there other Federal laws that require facility owners and operators to share information with first responders? I am referring to the Toxic Substances Control Act, CERCLA and Toxic Release Inventory reporting, the Emergency Planning and Community Right to Know Act, and the Clean Air Act's accidental release program.

RESPONSE: *Yes. Examples include, but not limited to:*

- *EPA Emergency Preparedness and Community Right to Know Act (EPCRA) Section 304: Emergency Notification*
- *EPA EPCRA Section 311: Safety Data Sheets (SDSs)*
- *EPA EPCRA Section 312: Tier I, II*
- *EPA EPCRA Section 313: Toxic Release Inventory (TRI)*
- *EPA Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) Section 103: Release Reporting*
- *EPA Clean Air Act Section 112(r): Accidental Release Prevention, Risk Management Program*
- *EPA Toxic Substances Control Act (TSCA) Section 8: Chemical Data Reporting*
- *DOT Hazardous Materials Regulations, 49 CFR Parts 171-180: Emergency Response and Release Reporting*
- *OSHA Hazard Communication Standard, 29 CFR 1910.1200*
- *OSHA Hazardous Waste Operations and Emergency Response (HAZWOPER) Standard, 29 CFR 1910.120*
- *OSHA Process Safety Management (PSM) Standard, 29 CFR 1910.119*

c. Is it true that biggest difference between CFATS and those other laws I just mentioned is that CFATS requires creation and production of documents about how the chemicals are protected from theft or diversion?

RESPONSE: *Yes. The CFATS program steps include: identifying threats, vulnerabilities, assessing risk, and applying countermeasures. The specific information derived from this process, for all facilities, could result in a "play book" for any adversary to circumvent the security measures that result from the approach. An analogous approach is often referred to as "Operational Security" or OPSEC. Essentially, this is a systematic method used to identify, control, and protect critical information and subsequently analyze actions associated with security activities to protect your information and activities from those with nefarious intent (criminals, terrorists, etc.)*

d. Would it concern you if this information was being shared more broadly than it is now?

RESPONSE: *Yes. See rationale above*

i. How so?

RESPONSE: *See rationale above.*

ii. What about as it relates to risks to the facility and the surrounding community?

RESPONSE: *The security measures implemented at facilities also protect the surrounding community from the risk of the highest consequence scenarios.*

2. Some have argued that DHS should be required to verify information submitted by a CFATS-covered chemical facility before lowering that facility's high-risk tiering or removing them from the program.

a. Do you think this is necessary?

RESPONSE: *I agree that this could be a needed step, although DHS should be able to implement a random selection approach or less than 100% inspection approach to account for resource constraints.*

b. Should DHS be required to verify information before increasing a facility's tier?

RESPONSE: *Yes. Historically, DHS' risk tiering methodology has been a bit of a "black box" with inconsistent outputs from nearly identical tiering inputs. DHS should be more transparent when it comes to tiering decisions. The site security*

management should be included in tiering decisions that affect his facility and personnel. And it is, in fact, the site security manager who has the ultimate responsibility for making critical security management decisions.

3. H.R. 3256 removes the factor of "practicality," making it an absolute requirement that CFATS facility owners and operators consult with their employees on vulnerability assessments and site security plans. In addition, the legislation compelling those consultations to recordkeeping rules and insisting that DHS base approval of a site security plan on the level of employee participation and input – rather than meeting the risk-based performance standards.

    a. Is there a general rule to how facility owners and operators interface with their employees on this kind of thing (i.e. collective bargaining)?

    RESPONSE: *Security planning is a multi-discipline undertaking. It requires the combined expertise of professionals in: security, human resources, legal, manufacturing operations, environmental, health services, safety and others. In addition, planning should involve employees at all levels. The main difference is the exposure of sensitive information consistent with the practice of "need to know" to maintain the OPSEC discussed above. For example, there is minimal need to discuss the details of cybersecurity to a warehouse inventory specialist unless her role has relevant cyber risk associated with it and her awareness of those threats and vulnerabilities bring value to the plan. Conversely, the cybersecurity professional has minimal need to know the detailed location of chemical inventories in the warehouse.*

    No distinction is or should be made on the responsibility to share information with stakeholders based on their status as a collective bargaining worker or not.

    b. Do you think "impracticable" consultations should be forced upon owners and operators?

    RESPONSE: *Absolutely not. This is inconsistent with the risk-based approach that makes the CFATS program so successful. Further, it does nothing to strengthen the security controls of the facility and introduces additional administrative burden and resource needs.*

    c. What is the practical effect of an absolute mandate of this kind on smaller facilities and facilities with contentious labor situations?

    RESPONSE: *Smaller facilities have fewer resources to comply and would potentially need to make unwanted trade-offs for compliance. In other words, they would have to pick and choose which elements of the regulation to spend more effort on. The documenting of who was involved in the planning along with the "collective bargaining" requirement begins to outweigh the non-prescriptive but*

higher value actions of the regulation.

4. Questions about the Personnel Surety (or identity verification against the Terrorist Screening Data Base for the lay people) have constantly been an issue with CFATS. After having finished with the highest risk, high risk facilities – Tiers 1 and 2; DHS is now implementing these requirements at the lower risk, high risk facilities – Tiers 3 and 4 – which are the lion's share of CFATS regulated facilities.

    a. How should DHS handle these facilities regarding personnel surety?

    RESPONSE: *Very little is known about what benefit there has been from DHS' implementation of personnel surety for tiers 1 and 2. What conclusions can be drawn regarding benefit-cost analysis? What validation does DHS see regarding the risk of sharing sensitive personal identifying data? There also remains a high level of uncertainty and skepticism on the part of industry on whether DHS would promptly notify the company of a positive hit on the TSDB. DHS and other authorities should involve industry personnel in positions of trust with the follow-on actions after a positive hit.*

    ACC members implement a host of background checks on its personnel as required by CFATS and independently based on company/industry standards. In addition to checking for terrorist ties, CFATS requires criminal background checks, verification of identity and legal U.S. employment verification. The incremental benefit associated with terrorist screening, compared to the cost and time of collecting, protecting and managing personal information on hundreds and thousands of employees and contractors is questionable. In addition, the increase in security vulnerability of sending that information over the internet to DHS seems to outweigh any incremental value.

    b. Would relaxing background checks at these facilities encourage terrorists to target them? Why?

    RESPONSE: *All CFATS facilities should be required to conduct criminal background checks, employment verification and identity. However, terrorist screening should be optional for lower risk Tiers 3 and 4, for the reasons stated above. .*

    DHS should conduct a complete cost-benefit analysis to demonstrate that the value of terrorist screening outweighs the costs. As they currently have not implemented at Tiers 3 and 4, this would not constitute a "relaxing" of security checks at facilities.

    CFATS facilities employ a host of security layers to protect their assets including security guards, background checks, monitoring and access control. Each of these layers of protection provide a substantial deterrent to would-be terrorists. As

such, CFATS facilities present a highly hardened target, which is why we haven't seen a terrorist attack on a chemical plant in the United States. Unfortunately other mechanisms are in place today that make it far too simple to purchase hazardous chemicals over the internet from China. The Federal Government should focus its attention and resources on protecting our communities from real risks.

5. CFATS recently updated its risk methodology to incorporate all the elements of risk contained in the National Infrastructure Protection Plan definition of risk: vulnerability, threat, and consequence.

    a. H.R. 3256 seeks to have this methodology redefined. Is this a good idea?

    RESPONSE: *The current risk methodology is consistent with the NIPP definition of risk and has produced a more accurate and more consistent result. We are unaware of why this change is being sought and what deficiency it is trying to fix. It does not need to be changed.*

    b. What is the practical effect of changing the definition of risk and why would it be a bad idea?

    RESPONSE: *Any substantive change to the definition of risk would initiate a complete re-tiering of hundreds, if not thousands of facilities. This type of upheaval is unnecessary and would create extreme uncertainty in the regulated community. Again, it is not clear what problem is being solved by such a radical departure from the traditional definition of risk.*