

Before the

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY

UNITED STATES HOUSE OF REPRESENTATIVES

Statement of

Timothy J. Scott

Chief Security Officer and Corporate Director

Emergency Services and Security

The Dow Chemical Company

Representing

The American Chemistry Council

On

The Chemical Facilities Anti-Terrorism Standards Program:

Addressing Its Challenges and Finding a Way Forward

Tuesday, March 6, 2012

Chairman Lundgren, Ranking Member Clarke and members of the subcommittee, my name is Tim Scott and I'm the Chief Security Officer of The Dow Chemical Company. I'm speaking today on behalf of Dow and the American Chemistry Council, the nation's largest chemical industry trade representative.

I'll focus on 4 points today:

First – there clearly are concerns on all sides about the lack of progress on the implementation of the CFATS program. This poses a growing concern to both industry and this subcommittee, but we see these as management issues – not issues with the CFATS concept.

Second – the members of the American Chemistry Council implemented the Responsible Care Security Code in 2002 and have voluntarily and significantly improved the security of its member facilities over the past decade. Since the Security Code's inception ACC members have spent nearly 10 billion dollars on security enhancements. We have worked with DHS from the beginning to make CFATS successful.

Third – in spite of the apparent issues the Chemical Facilities Anti-Terrorism Standards have made some progress toward improving the security of our nation's chemical sector since the implementation of the program – the concept and design of CFATS are good.

And fourth – we now have an excellent opportunity to correct the course and complete the critical task before us.

The concerns associated with the implementation of the Chemical Facilities Anti-Terrorism Standards (CFATS) – along with the apparent internal issues at DHS -- are disheartening, but not a cause for altering our course and nullifying the effort and progress that have been made. What started as a strong and successful public-private partnership with robust communication and collaboration that made the initial CFATS initiative successful clearly has declined. With that decline came the stagnation of the program and progress. This is not a condemnation of everyone and everything in DHS - there are many good people in DHS doing their best and doing a good job – this is a breakdown in management, communication and collaboration making a relatively straightforward program overly complex and burdensome.

This is a wake-up call – not a death knell. We now have the catalyst for change and an excellent opportunity to correct the course and complete the task at hand.

The concept and basic design of CFATS are solid. CFATS has potential, has already sparked some improvements in chemical security and can be developed further into an efficient, productive process to improve the security of our nation's critical chemical industry. Industry has dedicated billions of dollars on security since the implementation of CFATS. We've spent thousands of hours working with DHS at every level.

I would like to point out what Dow Chemical alone has done in terms of capital investments and security upgrades in an effort to lead the industry in compliance with the CFATS program. Dow has spent approximately \$250 million on security systems to ensure our facilities are as safe and secure as they

can reasonably be and we have completed vulnerability assessments, audits and as needed security upgrades at our facilities worldwide – not just those regulated under CFATS in the US. We did this in part because we have a duty to our shareholders, employees, and communities but also because we find the CFATS program a good model – in harmony with the Responsible Care Security Code -- to secure our facilities. It's my understanding that Dow is the only chemical company to achieve SAFETY Act designation from DHS for both our site security and our distribution system security processes.

The concept is good – risk-based and focused on the right priorities. The design of the CFATS program is good – allowing the regulated companies to apply customized security systems and processes to each unique site and situation in compliance with the DHS-established risk-based performance standards and DHS approvals. What's wrong or misguided with CFATS are in the details and those can be fixed if we work as a collaborative team with a common goal. We need to fix what's wrong, but not start over from square one.

There are many effective and efficient options that can achieve the successful implementation of CFATS as well as the ultimate goal of reducing the vulnerability and mitigating the risk of the chemical industry, our communities and our country. Working together we CAN get site security plans approved. We CAN get the highest risk sites audited. We CAN get agreements and plans in place designed to reduce vulnerabilities and comply with the risk-based performance standards. And this CAN happen within a very reasonable period of time. I've included with my written statement examples of potential solutions to many of the issues that in our opinion are the areas of most significant concern – the proposed personnel surety process, site security plan approval, transparency on the risk assessment process, and reasonable alternatives for site security plans and inspections that would expedite the process.

Attached to this written statement are examples of potential solutions to some issues of most concern – the personnel surety process, site security plan approval, transparency of on the risk assessment process, and reasonable alternatives that would expedite the process overall.

This will be a difficult task, but not an impossible mission. CFATS can work as conceived – implementation will take leadership, communication and collaboration well beyond what we've seen recently. We – DHS, the industry and this subcommittee – can make this work.

ACC has historically and consistently taken a proactive approach to security – establishing the Responsible Care Security Code in 2002 and supporting legislation to address and improve security across the chemical sector as a whole -- and have worked in good faith with DHS. Our members have aggressively stepped out to make significant investments in site security. Industry does not want to waste this effort by starting over.

ACC is ready and willing to take on the challenge as an equal stakeholder to finish the task and fully implement CFATS. We need DHS on the team to meet this challenge with a common mission and goal as they were when we started this journey and our early successes were achieved.

ACC asks that you separately address any internal issues in DHS and that you reauthorize the CFATS legislation so we can continue the efforts that are already well under way to secure our nation's chemical sector.

Tuesday, March 6, 2012 - Oversight Hearing Titled:

“The Chemical Facilities Anti-Terrorism Standards Program: Addressing Its Challenges and Finding a Way Forward”

Addendum to Testimony on behalf of:

- Timothy J. Scott, Chief Security Officer and Corporate Director, Emergency Services and Security, The Dow Chemical Company
- The American Chemistry Council

Recommendations for Consideration by:

The SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION AND SECURITY TECHNOLOGIES OF THE COMMITTEE ON HOMELAND SECURITY UNITED STATES HOUSE OF REPRESENTATIVES.

Dear Members:

The following are specific recommendations for your consideration that are intended to help improve the implementation of CFATS. With the guidance and oversight of Congress, many of these improvements could be achieved through administrative changes by DHS.

Personnel Surety:

DHS has been unable to implement a workable personnel surety program for CFATS facilities to properly vet thousands of employees and contractors against the Terrorist Screening Database. DHS can address this issue in two ways.

- (1) Begin accepting information of non-vetted employees at CFATS facilities for TSDB screening.
- (2) Leverage the existing Transportation Worker Identification Credential (TWIC) program by fully recognizing TWIC card holders as satisfying the TSDB screening requirement.

CFATS facilities can validate TWICs using existing tools such as the TSA’s Cancelled Card List without the need to collect, protect and transmit sensitive workers’ personal information to DHS.

While we recognize some shortcomings in the TWIC program, TSA continues to make improvements that will further strengthen the program. There are currently more than 1 million TWIC card holders. Most of them also work at CFATS sites. By simply leveraging the TWIC program fully, DHS could vastly improve personnel surety at CFATS facilities and greatly reduce the burden to the regulated community.

As a long-term goal, DHS should consider creating an enhanced vetting and credentialing program that incorporates the lessons from the TWIC program and has broader application across the critical infrastructure sectors.

Site Security Plan (SSP) Process:

DHS should engage members of the CFATS regulated community and their trade group representatives at the earliest stages and throughout the process to improve/revamp the SSP portion of CSAT. As identified in the “Memo”, this has been one of the biggest road blocks in DHS’s ability to efficiently

analyze and approve site security plans. However, this will be a long term effort to ensure it is done properly and will likely take several months to complete.

As an interim measure, ACC recommends that DHS work with the regulated community to accelerate the development of Alternate Security Programs (ASPs). ASPs can be developed in a relative short time frame, providing a standardized and consistent approach for plan submissions and approvals. ACC began such an initiative with DHS in November 2011 and plan to have the first ASP Guidance Document ready for use by this spring.

CFATS Program Transparency:

DHS should improve the transparency of the CFATS program by offering confidential sharing (in a classified setting if necessary) of pertinent facility-specific DHS risk information with the owner/operator. Facility owners/operators want to make fully informed decisions about managing their risks and implementing security measures. Currently the facility is unaware of how CFATS risk tiering decisions are made by DHS and how changes by the facility could reduce their risk and lower their CFATS profile. By making this process more transparent, it would vastly improve the security awareness of the facility and could identify potential tiering errors or anomalies before they arise.

Alternative Inspection Program for Tier 3-4:

DHS should consider an alternative self-inspection program for lower tier facilities (Tiers 3 & 4) using accredited third-party auditors. This alternative inspection program could be monitored with statistical sampling (audit schedule) by DHS CFATS inspectors to verify compliance. This would help streamline the program by lessening the burden on the DHS inspection cadre and allow DHS to focus resources and attention on higher risk facilities (Tiers 1 & 2). Existing private sector programs could be leveraged under this concept including the Responsible Care Security Code Program, which is mandatory for membership in ACC and requires third-party certification by an accredited third-party auditor.