



Testimony of

William E. Allmond, IV
Vice President, Government & Public Relations
Society of Chemical Manufacturers and Affiliates

before the

House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, &
Security Technologies

on

The Chemical Facility Anti-Terrorism Standards Program:
Addressing Its Challenges & Finding a Way Forward

March 6, 2012

Good morning Chairman Lungren, Ranking Member Clarke, and members of the Subcommittee. My name is Bill Allmond and I am the Vice President of Government & Public Relations at the Society of Chemical Manufacturers and Affiliates (SOCMA) in Washington, DC. I am pleased to provide this testimony regarding progress made by the Chemical Facility Anti-Terrorism Standards.

Five and a half years ago, and working in a bipartisan manner, Congress enacted a comprehensive chemical security regulatory program, the Chemical Facility Anti-terrorism Standards (CFATS). Thanks to this bipartisan effort, the U.S. Department of Homeland Security (DHS) and regulated facilities are well down the road in implementing this important program.

Regrettably, DHS has stumbled in its implementation of the program by failing to put in place, among other things, basic management practices or effective leadership, both at the Division level and at high levels. The 2011 internal memorandum “Challenges Facing ISCD, and the Path Forward” issued by Penny J. Anderson and David M. Wulf of the Infrastructure Security Compliance Division (ISCD) regarding the process of implementation is sobering. It demonstrates the fact that a government agency without proper management can take a credible program legislated by Congress and then mess it up. However, as this Subcommittee and others assess the Department’s failures with the CFATS program, we should be reminded that it is the process or personnel that needs addressing, not the program itself.

Today we will explain why we remain supporters of the CFATS program—despite DHS’s management failings—highlight achievements as a result of the program, and recommend solutions moving forward. At the outset, though, we emphasize these key facts:

- This demanding program is now requiring over almost five thousand chemical facilities nationwide to develop and deploy meaningful security enhancements.
- Equally important, it has led over 2,000 facilities to voluntarily take steps reduce their risk profile sufficiently that they no longer warrant regulation under the program.
- This performance-based regulation protects facilities against attack without impairing the industry’s ability to remain innovative and to maintain some of the nation’s highest paying manufacturing jobs.
- Finally, the standards have teeth. The Secretary of the Department of Homeland Security has the authority to levy significant fines on a facility for non-compliance, and can even shut down a facility.

I. SOCMA is the Only U.S. Trade Association Dedicated Solely to Serving the Needs of the Specialty, Batch, and Custom Chemical Manufacturing Industry

A. SOCMA

For 91 years, the Society of Chemical Manufacturers and Affiliates has been and continues to be the leading trade association representing the batch, custom, and specialty chemical industry. SOCMA’s nearly 230 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.

ChemStewards® is SOCMA's flagship environmental, health, safety and security (EHS&S) continuous performance improvement program. It was created to meet the unique needs of the batch, custom, and specialty chemical industry, and reflects the industry's commitment to reducing the environmental footprint left by members' facilities. As a mandatory requirement for SOCMA members engaged in the manufacturing or handling of synthetic and organic chemicals, ChemStewards is helping participants reach for superior EHS&S performance.

B. SOCMA's Security Achievements to Date

Maintaining the security of our facilities has always been a priority for SOCMA members, and was so before September 11. 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 the ChemStewards initiative, SOCMA members were required to conduct security vulnerability assessments (SVAs) and to implement security measures.

SOCMA designed an SVA methodology specifically for batch, custom and specialty chemical facilities that was approved by the Center for Chemical Process Safety (CCPS) as meeting its requirements for an effective methodology. SOCMA members have spent billions of dollars and have devoted countless man-hours to secure their facilities and operations. These investments will naturally continue for the foreseeable future.

Many (though by no means all) SOCMA member company facilities are encompassed by the CFATS program. These facilities have completed their Site Security Plans (SSPs) and will eventually be inspected by DHS to verify the adequacy of those plans and their conformance to them. SOCMA has tried to actively engage with DHS to accelerate and continuously improve the implementation of the CFATS program, exploring new approaches to personnel surety and Alternative Security Programs.

Some of our member companies' other facilities comply with the Coast Guard's facility security requirements under the Maritime Transportation Security Act (MTSA).

Looking well beyond regulatory requirements, our members have also partnered with DHS on many important voluntary security initiatives and programs through the years, including the Risk Assessment Methodology for Critical Asset Protection (RAMCAP), the Buffer Zone Protection Plans, and the Homeland Security Information Network (HSIN). SOCMA is a founding member of the Chemical Sector Coordinating Council, which has served as a model for how critical infrastructure sectors should work together and with DHS.

SOCMA also works jointly with DHS in organizing and financing an annual Chemical Sector Security Summit and Expo, a hugely successful, free event that brings together government

representatives, chemical security experts, and industry professionals to share knowledge and best practices to regulated and nonregulated facilities alike.

Through the Sector Council and other avenues, we and our members have developed close and open working relationships with DHS and other federal agencies, and with state and local governments, to exchange information and coordinate roles in maintaining the security of our critical chemical facility infrastructure. In particular, we have sought to engage continuously and constructively with ISCD, even though we could never gain much understanding of its internal operations. As the Anderson/Wulf memorandum reveals, we understood it far less well than we imagined.

II. Despite Departmental Mismanagement, CFATS is Reducing Risk and ‘Must Evolve’

SOCMA wishes to emphasize that we regard the program thus far as a success, even if its implementation is moving much more slowly than we all would prefer. The CFATS statute was wisely drafted to be comprehensive, appropriately performance-based, 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. The regulatory program they created is not inherently impossible for a government agency to implement, but it does require (i) knowledgeable people to review SSPs and inspect plants, and (ii) the courage to make decisions based on judgment. Unfortunately, the memorandum indicated that DHS’s ISCD staff largely do not have adequate expertise or training, in part because higher levels of the Department prevented them from being able to hire sufficiently expert personnel.

Since the program was launched in 2007, over 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 who 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.

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.

It is important to note that the memorandum that we all have now reviewed was not intended to highlight these achievements under CFATS; it was only meant to be an internal tool for ISCD’s

leadership to assess and subsequently respond to the immediate challenges to the program's implementation. The memo overwhelmingly and repeatedly points to process deficiency as a cause of DHS's failure to properly implement CFATS. In fact, DHS specifically states on page 10 of its memo that, "even with sufficient planning and vision it is a given that the implementation of a new program will naturally result in some mistakes and course corrections. The program must evolve."

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. The memo details the many things not being done by DHS. However, the industry has done a lot. Covered facilities have invested billions of dollars in security upgrades to meet CFATS's requirements. 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 since the inception of the program. CFATS has provided to significant additional security to a critical segment of our nation's infrastructure, as well as the general public – although, it is admittedly difficult to assign a monetary value to this increased security for purposes of justifying the program's annual cost to taxpayers.

Facilities with high-risk chemicals are safer today both because of CFATS and the efforts taken by industry by their own initiative. After 9/11, and prior to DHS's issuance of the risk-based standards, many companies already began proactively instituting security measures at their high-risk facilities. However, there were no uniform standards for measuring and implementing these security improvements across industry. CFATS has standardized the security process, but has allowed the voluntary assurance of chemical security to continue through DHS's Voluntary Chemical Assessment Tool (VCAT). The Chemical Sector Specific Agency developed VCAT to assist additional facilities that fall outside CFATS to assess their own risks and to implement voluntary security measures as desired. SOCMA has endorsed VCAT through our ChemStewards® EHS&S management program, in which participation is mandatory for all active members.

No one should dispute that, despite the challenges to its implementation, the two main alternatives to CFATS – no chemical security regulations at all, or a prescriptive program that places such burdens on industry as mandatory incorporation of inherently safer technology (IST) and would subsequently threaten to drive chemical operations overseas where security standards are weaker – would both be far worse. Since the program's inception, no terrorist attacks have taken place in the United States that involved chemicals or that would otherwise indicate that CFATS has failed its purpose.

III. CFATS Implementation Challenges are Not Insurmountable.

The internal problems holding back CFATS implementation are serious and significant but not insurmountable. SOCMA is confident that the new leadership of Penny Anderson and David Wulf is committed to improving its programmatic implementation. Thanks to the internal assessment, they a greater understanding of the challenges facing them and a robust action plan.

SOCMA is also committed to working with the Department to improve its implementation, where appropriate. The industry has nothing to gain from this crisis. And we have been concerned about the slow pace of implementation for years. First, delays create uncertainty. Regulated businesses do not like to hang in suspense for years wondering if their major capital commitments were sufficient. Second, delay only invites negative stories in the press, like the ones we are now starting to see, questioning the security of chemical plants -- when we know that these facilities have done what they have been asked or required to do at this stage. Delays can also make companies believe their government is not really serious about the security of chemical facilities. It is hard to believe DHS is serious, when commitments made about approving SSPs and completing pre-authorizing inspections are repeatedly broken. Such failures cause security professionals to lose credibility with their superiors who authorize compliance costs, as these managers conclude that their security staff are simply “crying wolf” about their regulatory obligations. DHS mismanagement has, in some cases, stopped the forward momentum that security managers had with their own senior management in convincing them of the need for certain cost decisions, placing forward progress in a holding pattern.

The following are SOCMA’s recommendations for placing CFATS implementation back on track:

A. Congress Should Encourage ISCD to Embrace Greater Collaboration with Industry to Enhance Public-Private Partnership

The CFATS framework is sound; however, DHS’s implementation has been flawed. This is largely because DHS has drifted away from the spirit of the public-private partnership on chemical security that it has so often hailed as a keystone of the CFATS program. Congress should encourage ISCD to work collaboratively with the regulated community to solve the technical, training and tool-related issues currently presenting challenges to the implementation of CFATS.

Industry can provide much assistance moving forward, including ways for DHS to minimize the future cost and complexity of the CFATS program. For example, the Chemical Sector Coordinating Council (CSCC), the industry advisory body that interacts with DHS on security issues, over a year ago presented DHS with a viable and immediately implementable personnel surety proposal that addresses the many shortfalls of the Department’s own proposed program. DHS’s current proposal, which is under review by the Office of Management and Budget, places unreasonable reporting and information-gathering burdens on regulated sites, does not leverage the use of existing federal credentials that already screen candidates against the very same background check requirements as proposed in the pilot, is overly prescriptive and does not reflect the flexible framework of the CFATS standards themselves.

B. More Operational Transparency Is Warranted

ISCD can safely be much more transparent about its operations. While some classified information and chemical-terrorism vulnerability information (CVI) should not be disseminated, there is no reason why ISCD cannot communicate the progress of its operations more clearly and regularly to both Congress and the public. The tremendous change that the new ISCD leadership

wants to drive will never occur unless ISCD reports regularly to Congress. More sustained oversight will enable Congress to hold DHS accountable going forward, so the mistakes of the past are not repeated or perpetuated.

C. Simplifying Personnel Surety and Federal Background Check/Credentialing Programs

Congress should assure itself both that the CFATS program continues to be effective and that DHS and other agencies minimize duplication and unnecessary regulatory burdens. A prime example is the personnel surety program that DHS is developing under CFATS. Risk-Based Performance Standard #12 requires facilities to implement security measures designed to: (i) verify and validate identity; (ii) check criminal history; (iii) verify and validate legal authorization to work; and (vi) identify people with terrorist ties. The facility is responsible for the first three tasks and for determining what criminal background findings would be disqualifying. Evaluating terrorist ties requires federal government involvement however, in the form of evaluating names against the national Terrorist Screening Database (TSDB) maintained by the FBI.

DHS has announced its intent to establish a web-based application that would require facility owners and operators to submit personally-identifying information about current and prospective employees, as well as contractor and visitor personnel seeking access to a plant.¹ Our industry has expressed serious reservations about this proposal, in part because of the heavy presence of contractors at chemical sites, especially during plant-wide maintenance “turnarounds.” In particular, we have strongly urged DHS to rely on the half-dozen or so other federally-issued credentials that involve a TSDB check. Unions have also expressed concern about DHS’s proposal.

DHS has been open to discussing alternative approaches, and the industry has proposed both interim and long-term alternatives that could involve reliance on existing federal vetting programs (e.g., the Transportation Worker Identification Credential or TWIC), mechanisms by which contractor and visitor employers could submit information regarding their own employees, and ultimately a universal federal security credential that would supersede all others.

While we have had productive discussions with the Office of Infrastructure Protection on our proposals, any alternative has had to struggle against (i) the desires of some within DHS to make CFATS a system for tracking who has ever had access to which chemical facility, and (ii) resistance within TSA to allowing TWICs to be made available to persons working in non-maritime settings. We realize that these issues fall into the jurisdictions of multiple congressional committees. Especially for that reason, we urge this subcommittee and others with jurisdiction to work together, and with DHS and other agencies, to minimize the burdens of assuring personnel surety under the CFATS program and, more generally, to rationalize the current crazy quilt of security credentialing programs. Resolving this challenge expeditiously would free up ISCD resources to focus on the more pressing tasks of approving SSPs and

¹ See 76 Fed. Reg. 34729 (June 14, 2011).

initiating compliance inspections.

D. Mandating Inherently Safer Technology into CFATS Program Is the Last Thing ISCD Should—Or Even Could—Implement

As the memorandum clearly points out, ISCD staff are substantially lacking in knowledge and expertise even about security, much less chemical process safety. They have shown great reluctance to make decisions on relatively simple issues like physical security. It is obvious to SOCMA that they are even more unqualified to make much more sophisticated and decisions about process safety. Congress should thus not devote any further time to discussing the discredited concept of mandatory IST.

An IST mandate such as that contained in last year's House bill would have created a new CFATS statute to require Tier 1 and 2 facilities to implement "methods to reduce the consequences of a terrorist attack" – i.e., IST – whenever DHS made specified findings about risk reduction and technical and economic feasibility. However commonsense such a mandate might appear on the surface, it is fundamentally a bad idea in the security context. Inherent safety is a superficially simple but truthfully very complex concept, and one that is inherently unsuited to regulation. It could also wreak economic havoc on regulated facilities, notwithstanding the findings DHS would have to make.

First and foremost, it is important to clarify a common misunderstanding about inherent safety. Quite simply, IST is a process-related engineering concept, not a security one. It is premised on the belief that, if a particular chemical process hazard can be reduced, the overall risk associated with that process will also be reduced. In its simplicity, it is an elegant concept, but the reality is almost never that simple. A reduction in hazard will reduce overall risk if, and only if, (i) that hazard is not displaced to another time or location and (ii) it does not result in the creation of some new hazard.

Inherent safety is only successful if the sum total of all risks associated with a process life cycle is reduced. This is rarely a simple calculation, and to some extent it is an irreducibly subjective one (for example, a substitute chemical that may reduce explosion risks may also pose chronic health risks). The calculation becomes even more difficult when it is being done not solely for reasons of process safety (where accident probabilities can be estimated with some degree of confidence) but also for reasons of security (where the probability of terrorist attack is highly uncertain but certainly low). Finally, there is no agreed-upon methodology to measure whether one process is inherently safer than another process. For all these reasons, the world's foremost experts in IST and chemical engineering have consistently recommended against regulating inherent safety for security purposes.

E. ISCD Needs to Retrain and Potentially Replace Much of Its Staff

Furthermore, it is evident from the memorandum that ISCD needs to retrain and may need to replace much of its staff. ISCD's Penny Anderson and David Wulf are exceptions, however. They are not responsible for the situation they inherited. Writing the kind of memorandum they authored shows that they are experienced, capable government managers who know what needs to be done. They are going to need a lot of help, however, including continued congressional

oversight to make sure they are getting the cooperation they need from DHS management and from the union.

For others within ISCD, though, the memorandum makes clear that too few experienced staff bear the bulk of the responsibility for the administration of CFATS, and far more do not know how to conduct their work or even have properly defined position responsibilities; others simply have an unrealistic view of their jobs.

Congress should examine DHS's hiring guidelines and practices to eliminate the identified obstacles to the recruitment and retention of qualified staff for the CFATS program. Replacing and retraining staff may result in immediate costs to the Department in the short term, but would lead to long term savings through the reduction of ISCD's reliance on contractors, which the memorandum found cost a great deal more than Federal employees. Additionally, relying on contractors who typically have high job turnover precipitates the need for constant retraining. Institutional knowledge is lost when key activities are conducted primarily with contract support.

F. Congress Needs to Provide Certainty for Regulator and Regulated Alike By Approving a Multiyear CFATS Reauthorization

The memorandum identifies the failure to achieve long-term or permanent authorization of CFATS as one of the greatest challenges to the program's future success. It may appear counterintuitive to advocate for long-term authorization of a troubled program, but the key to fixing CFATS is vigorous oversight, not budgetary uncertainty or budget cuts. SOCMA continues to support a long-term extension of the standards to allow DHS and the regulated community to come fully into compliance.

IV. Conclusion

Moving forward, if DHS is to suitably engage industry and be accountable for its progress, Congress conducts regular oversight, and the program is provided regulatory certainty, SOCMA believes that CFATS can successfully be implemented without the need for additional legislation.

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