October 17, 2014

U.S. Department of Homeland Security
National Protection and Programs Directorate
Office of Infrastructure Protection, Infrastructure Security Compliance Division
245 Murray Lane, Mail Stop 0610, Arlington, VA 20528-0610

RE: 6 CFR Part 27; Chemical Facility Anti-Terrorism Standards, Advance notice of proposed rulemaking, [Docket No. DHS-2014-0016] RIN 1601-AA69

ACC and its members appreciate this opportunity to submit information and recommendations on improving the Chemical Facility Anti-Terrorism Standards (CFATS) regulatory program. ACC supports this rulemaking process as a step towards advancing the CFATS program and identifying ways to make the program more effective.

While ACC and its members agree that a periodic review is necessary for the continued success of the CFATS program, ACC believes there are significant issues that could be addressed that do not require formal rulemaking, and can be corrected through technical changes. We encourage the Department of Homeland Security (DHS) to address the issues raised in our comments.

Chemical Security Assessment Tool (CSAT):

One of the primary roadblocks to effectively and efficiently implementing the CFATS program has been the web-based interface developed by the Department called CSAT (Chemical Security Assessment Tool). The initial concept of CSAT was to automate and streamline the data collection and assessment function for the CFATS program. While the concept of CSAT was commendable, the reality is that CSAT has not functioned well. Minor improvements have been made, such as adding page numbers to reports, pre-populating Site Security Plan (SSP) survey questions and adding commas to numeric fields. While these edits have been helpful, the structure, format and functionality of CSAT still needs more work.

For example, the CSAT process is unnecessarily complex. Site Vulnerability Assessments (SVAs) are being used simply as an information collection tool (survey), but much of the required analysis is done in the Site Security Plan (SSP) step. In ACC's view, corrections and simplification in the SVA module could focus the SSP step on specific actions implemented to reduce vulnerabilities in a manner suitable for verification and auditing. A concise and focused

SSP could also help set the stage for considering the use of third party audits as a means of demonstrating CFATS compliance.

Users of CSAT are required to submit much information that is not necessary for implementing the CFATS program. Duplication and redundancy is apparent throughout the various CSAT modules. Furthermore, the CSAT end products generated by the Top-Screen, SVA and SSP modules return little value for the owner/operator in addressing their site security. ACC and others have developed Alternative Security Programs (ASPs) to help streamline the SSP process to identify meaningful site security improvements. Other streamlining enhancements have included the adoption of a Corporate Review Process that prioritizes and leverages inspections to make the most effective use of time and data for multiple facilities with a common owner, where security plan elements are not unique to a specific facility. ACC believes the ASP approach provides an important alternative to CSAT for owners/operators as well as DHS.

ACC strongly recommends that DHS overhaul the CSAT system. Input already received from the CSAT user community, chemical security professionals, DHS inspectors and DHS headquarters staff who rely on CSAT to implement the program should be incorporated into such a major modification of CSAT. We also encourage DHS to further promote the use of ASPs.

Lastly, DHS should process top-screens, security vulnerability assessments (SVAs) and SSPs/ASPs within a prescribed timeframe. The CFATS regulation requires facilities to submit Top-Screens, SVAs and SSPs/ASPs within specific timelines (e.g., within 90 days of receiving notification from DHS). Conversely, DHS does not have deadlines for its review and adjudication. As a result, facilities may submit timely filings via the CSAT but do not receive a DHS response for months – or even years. This delayed review can hamper a facility's ability to appropriately plan, design, and implement security projects to comply with CFATS and affects confidence in the CFATS program overall.

Industry Programs:

DHS should leverage industry security programs, such as ACC's Responsible Care Program, to help effectively manage and accelerate the CFATS implementation schedule. Congress recognized the value of these programs when it passed section 550 of the DHS Appropriations Act of 2007 by providing DHS the ability to adopt industry developed ASPs on a broad basis. Members of the CFATS community who are in compliance with an industry security program and who can demonstrate such through a third-party auditor should be put on an accelerated track for review and approval. This would help distinguish those owner/operators who have been proactive by investing in security measures well in advance of DHS oversight from those who

may need serious compliance assistance. This would provide DHS the ability to prioritize their reviews and inspection process and focus on those sites that need help with implementation.

Personnel Surety:

ACC is particularly concerned about the lack of a functional vetting process for owner/operators to submit information on personnel for vetting against the Terrorist Screening Database (TSDB). While owner/operators are able to conduct criminal background checks, verify identity and eligibility to work, the federal government is the only entity that can vet against the TSDB. TSDB vetting is one of the most significant elements of the CFATS program under CFATS Risk Based Performance Standard 12. While other security programs such as the U.S. Coast Guard Maritime Transportation Security Act (MTSA) long have had terrorist screening procedures in place, DHS has not adopted these programs for use by the CFATS community.

One simple technology solution that DHS should adopt is to create a secure public website that allows individuals to submit their own information directly to DHS for vetting against the TSDB. A web-based technology solution could significantly reduce the burden on regulated facilities while enhancing security.

In the absence of a complete CFATS Personnel Surety Program, ACC members are willing to voluntarily submit information to DHS (protected under Chemical-Terrorism Vulnerability Information {CVI} protection regime) on their employees and contractors who require access to restricted areas of covered facilities for vetting against the Terrorist Screening Database. ACC and its members would welcome an opportunity to work closely with DHS to develop a process for the voluntary submission of information.

Risk Tiering and Transparency:

On October 8, 2013 the Homeland Security Studies and Analysis and Institute (HSSAI) published its final report on a peer review of the Chemical Facility Anti-Terrorism Standards tiering methodology. The Peer Review Panel was established in 2012 as a result of identified data errors being generated by the CFATS risk tiering methodology that become public in 2010 and 2011. During early 2013, the Expert Peer Review Panel reviewed the CFATS risk tiering methodology and made several key findings including:

- The CFATS risk tiering methodology is inconsistent in how it assesses different types of risk.

- DHS should improve the transparency of the assessment methodology.
- DHS should revise the current tiering methodology.

In light of these findings, ACC and its members are concerned that CFATS implementation will continue to rely on a risk determination process acknowledged to create inconsistencies and uncertainties. While we appreciate that DHS is taking steps to address the problems, it may well be several years before the risk tiering process is improved.

ACC recommends that DHS accelerate the work of the panel to address the HSSAI report and be transparent in its findings. It is also important that DHS be transparent regarding the risk determining factors that cause a site to be ranked at a certain risk tier level. Currently, DHS does not share the determining factors of their risk tiering decisions with the covered facility. There is no process that facilitates dialogue between DHS and the site security personnel on the risk details, even under classified conditions. This is a major concern since the very people who have the most influence on the security – site owners/operators – are not provided risk information by DHS. ACC believes this is a significant flaw in the current CFATS program.

In a similar vein, DHS needs to do a better job of focusing their intelligence products on private sector needs. It is not helpful for a security manager to receive classified information mixed in with For Official Use Only (FOUO) and unclassified information, and then face limitations on what can be shared with other relevant personnel at a facility.

Risk Based Performance Standards:

Many of the Risk Based Performance Standards (RBPS) are repetitive, address the same concepts and should be consolidated and/or combined. For example, RBPS 4 (Deter, Detect, and Delay) should be consolidated into RBPS 1 (Restrict Area Perimeter), RBPS 2 (Secure Site Assets), and RBPS 3 (Screen and Control Access). RBPS 4 requires facilities to "[d]eter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful...." A majority of the concepts in RBPS 4 are concepts that are already addressed in RBPS 1, RBPS 2, and RBPS 3. This is evidenced, among other places, by DHS's Chemical Security Assessment Tool (CSAT) and Site Security Plan (SSP), which prompts facilities to answer many of the exact questions in RBPS 4 that they previously answered in RBPSs 1, 2, and 3 (including questions regarding security patrols, security posts, and closed-circuit television). RBPS 4 questions not already addressed in RBPSs 1, 2, or 3 (such as vehicle barriers and key control) are better suited for, and should be included in, RBPS 1 and RBPS 3, respectively.

There are other RBPS's that could be combined as well, such as RBPS 13 (Elevated Threats) and RBPS 14 (Specific Threats, Vulnerabilities, or Risks) could be combined into one RBPS entitled "Specific and Elevated Risks."

RBPS 15 (Reporting of Significant Security Incidents) and RBPS 16 (Significant Security Incidents and Suspicious Activities) should be consolidated into a single RBPS. RBPS 15 requires facilities to "report significant security incidents to [DHS] and to local law enforcement officials" while RBPS 16 requires facilities to "identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site." As indicated in the RBPS metrics for each, RBPS 15 focuses on identifying and appropriately *reporting* significant security incidents while RBPS 16 focuses on *investigation* of significant security incidents and dissemination of lessons learned. Practically, the identification, reporting, and investigation of significant security incidents (as well as the associated recordkeeping and the dissemination of lessons learned) are too closely related to separate into discrete RBPSs. Indeed, when developing protocols to address RBPS 15 and RBPS 16, many companies do so using a *single* procedure.

Lastly, RBPS 17 (Officials and Organization) and 18 (Records) could be combined to address Administrative Issues.

For future implementation purposes, it would be important for DHS to develop a cross-walk of RBPSs that are eliminated or combined with others, so that facilities referencing older standards in their plans can make appropriate updates.

ACC also encourages DHS to provide example strategies (standard practices) for each RBPS that could meet the intent of the standard After several years of implementing the program and seeing what is being commonly employed at various sites in different industries, DHS should be able to provide some helpful illustrative examples for each RBPS. ACC believes this would be helpful for both DHS and industry as there will be new staff implementing the program, new sites implementing CFATS and this may save sites and DHS time.

ACC further recommends that DHS make clear that the example strategies are not mandatory, and do not represent the only acceptable compliance method. We note that the original draft RBPS guidance document contained compliance examples but were removed by DHS for fear they would be too prescriptive and in conflict with the risk based nature of CFATS. ACC believes that implementation experience to date could provide very useful suggestions on common practices, procedures and technologies, particularly for small and medium sized entities.

CFATS Inspection Process:

Much attention has been focused on the Department's efforts to satisfy its statutory and regulatory requirements associated with the review and approval of SSP in a timely fashion. In its April 2013 report on CFATS, the Government Accountability Office (GAO) estimated that it could take seven to nine years for the program to eliminate the backlog of reviewing facilities' site security plans and conducting compliance inspections. ACC believes that the Department has made notable progress recently in speeding up its review of security plans and conducting compliance inspections. We also believe it is necessary to expedite these reviews so that needed security measures are put in place as soon as possible.

ACC believes that the SSP approval backlog is largely attributable to the fact that DHS is conducting physical onsite facility inspections as a prerequisite to approving SSPs. We note that on-site inspections are not legally required, and it appears this has strained DHS resources.

ACC fully appreciates the importance of the security plan approval process and strongly supports DHS's efforts to conduct thorough reviews consistent with the Department's legal obligations and overall mission. ACC believes that various industry security programs exist that could be leveraged to expedite the CFATS inspection process and do so in a way that is consistent with governing law and security interests.

The CFATS authorizing legislation (Section 550 of the DHS Appropriation Act of 2007, Pub. L. 109-295) states:

> *[T]he Secretary may not disapprove a site security plan submitted under this section based on the presence or absence of a particular security measure, but the Secretary may disapprove a site security plan if the plan fails to satisfy the risk-based performance standards established by this section: Provided further, That the Secretary may approve alternative security programs established by private sector entities, Federal, State, or local authorities, or other applicable laws if the Secretary determines that the requirements of such programs meet the requirements of this section and the interim regulations: Provided further, That Secretary shall review and approve each vulnerability assessment and site security plan required under this section…*

While this section sets forth the broad parameters governing SSP approval, it does not require that an onsite facility inspection be conducted prior to the DHS Secretary approving a site security plan. Moreover, the section provides that the Secretary may approve ASP established by private entities.

Furthermore, the DHS Secretary's CFATS inspection authority is found in Section 550(e) of the act, which simply states:

> *"The Secretary of Homeland Security shall audit and inspect chemical facilities for the purposes of determining compliance with the regulations issued pursuant to this section."*

Importantly, this provision provides that the Secretary's authority to audit and inspect chemical facilities is limited to determining "compliance" with the CFATS regulations, as opposed to expressly authorizing an inspection for the purpose of determining whether a plan should be approved or disapproved. Section 550(g) of the CFATS statute, however, suggests that the sufficiency of a facility's SSP could be a factor in determining "compliance" with the CFATS regulations:

> *"If the Secretary determines that a chemical facility is not in compliance with this section, the Secretary shall provide the owner or operator with written notification (including a clear explanation of deficiencies in the vulnerability assessment and site security plan) and opportunity for consultation, and issue an order to comply by such date as the Secretary determines to be appropriate under the circumstances…"*

The CFATS statute imposes no obligation on DHS as to the circumstances governing when a compliance inspection or audit must be conducted (e.g., prior to SSP approval or after SPP approval to determine ongoing compliance), let alone the required elements of any such an audit or inspection (e.g., in-person site visits, conducting telephone interviews, or merely collecting documentary evidence confirming compliance). Therefore, nothing in the CFATS legislation expressly requires the inspection to be conducted prior to approving a SSP, nor does it require an "inspection" be conducted in-person. Rather, the CFATS statute broadly authorizes DHS to conduct inspections and audits solely for purposes of determining "compliance" with the CFATS regulatory scheme.

ACC recommends that DHS formally recognize verified compliance with industry security programs as a factor in the CFATS inspection and SSP/ASP approval processes. For example, DHS could determine that an ASP submitted by a facility deemed to be in compliance with the Responsible Care Security Code, or similar industry program, leads to a presumptive determination that the plan is sufficient for purposes of issuing a final Letter of Approval to the submitting facility. In lieu of conducting a physical onsite facility inspection, DHS could obtain and inspect the records of the facility to confirm compliance with third-party verification requirements, including any inspection reports or other evidentiary records supporting compliance. Even after approving the SSP/ASP, DHS would maintain clear authority to conduct an on-site compliance inspection at any time.

In determining whether an on-site inspection was required, DHS could also consider whether the facility ASP is based upon a security plan that has been previously approved by DHS, such as a security plan that the US Coast Guard approved under MTSA or DHS granting the plan SAFETY Act approval. DHS also has the authority to consider a facility's CFATS Tier Level in determining whether an onsite inspection is warranted. In ACC's view, DHS has significant discretion in determining how and when it will conduct inspections at covered facilities.

Conclusion:

We believe that ACC's recommendations, if implemented, would have a significant impact on the performance of the program, and instill greater confidence within the regulated community that DHS has the ability to effectively manage CFATS and help enhance chemical security. ACC looks forward to working with DHS to address the issues outlined in this document.

Please let us know if you have any questions. For more information contact Bill Erny, bill_erny@americanchemistry.com or 202-249-6412.

Sincerely,

William J. Erny **| American Chemistry Council**
Senior Director, Policy, Regulatory & Technical Affairs
bill_erny@americanchemistry.com
700 2nd Street, NE | Washington, DC | 20002
O: (202) 249-6412
http://www.americanchemistry.com