Statement for the Record
Robert B. Stephan
Assistant Secretary, Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security

Before the

Committee on Homeland Security
Subcommittee on Transportation Security and Infrastructure
United States House of Representatives

Tuesday, July 24, 2007
1:00 PM.
Room 311, Cannon House Office Building

Thank you, Chairwoman Jackson-Lee, Congressman Lungren, and distinguished members of the Subcommittee. It is a pleasure to appear before you today to discuss chemical security. Open dialogue between security partners is a key element in advancing the security of our nation, and I appreciate this opportunity to address you on such a timely and important topic. Securing the Chemical Sector represents an immense undertaking that involves a national effort including all levels of government, industry, and the public. Integrated and effective partnerships among all stakeholders – federal, state, local, and private sector – are essential to securing our national critical infrastructures, including high-risk chemical facilities.

The Chemical Sector and the Sector Specific Plan

The Chemical Sector has nearly one million employees and represents $500 billion a year in revenue. It converts raw materials into more than 70,000 diverse products, many of which are critical to the health and well-being of our nation's citizens, to security, and to the economy. The contributions the Chemical Sector makes to the Nation are great, but they are not without risk. The economic and strategic value of the industry may make it an attractive target for terrorists. Many chemicals, either in their base form or when combined with other chemicals, could cause significant harm to people and the environment if released or removed from a facility and weaponized in some fashion. Additionally, a terrorist attack, natural disaster, or industrial accident could significantly disrupt production at key facilities, causing supply chain issues that could be harmful to the economy on a regional, national, or global scale.

The Department of Homeland Security's (DHS') vision for the Chemical Sector is that of an economically competitive industry with a sustainable security posture. This can be achieved by using risk-based assessments, industry best practices, and a comprehensive information sharing environment between industry and government. This vision also includes the implementation of a tailored new regulatory authority – the Chemical Facility Anti-Terrorism Standards (CFATS) – aimed at securing the most high-risk sites around the country. It is the combination of voluntary industry efforts and risk-based public-private collaboration inside and outside of regulatory space that will enable implementation of this vision.

Industry Efforts

In the nearly six years since the terrorist attacks on September 11, 2001, the great majority of industry owners and operators have taken actions to assess facility vulnerabilities and put in place a wide variety of operational, physical, and cyber security measures. In fact, the Chemical Sector has invested more than $3 billion in voluntary security measures in the aggregate since 9/11. In our experience, Chemical-Sector owners and operators generally understand the importance of integrating security into their operations as a sound and responsible business practice.

Examples of industry-led protective initiatives include:

Responsible Care Security Code: There is a history of collaboration within the sector on chemical safety, most notably in the American Chemistry Council's Responsible Care program supported by key industry associations. After September 11, this program was modified to include a mandatory Responsible Care Security Code for chemical facility security which requires facilities to:

- Assess vulnerabilities using methodologies developed by Sandia National Laboratories or the Center for Chemical Process Safety.
- Implement security enhancements.
- Verify physical enhancements through local officials or third parties.

Specifically, facilities are required to control vehicular and pedestrian access to sites; protect the perimeter through physical barriers, access control systems, electronic surveillance, and patrols; create, train, and rehearse security plans; ensure backup for critical chemical process systems, including offsite control rooms; work with regional stakeholders (government and emergency services) to ensure timely response and communication; and vet and access clearance for employees and contractors. The Security Code has requirements for cyber security and transportation, as well.

Chemical Sector Cyber Security Program: The Chemical Sector Cyber Security Program was established by the American Chemistry Council (ACC). In April 2002, ACC recognized the need for a unified plan of action to address cyber security across the sector, as well as with technology providers, supply chain partners, and other critical infrastructure industries. To accomplish this, a task force comprised of 16 high-level subject-matter experts was chartered to create the *Chemical Sector Cyber Security Strategy*. This strategy was published in September 2006 and outlines the sector's plans to continue facilitating improvements to IT and manufacturing system security.

Sector Protective Programs: Several industry trade associations have developed risk assessments methodologies and technical tools to support their member companies. In fact, many associations require completion of risk assessments as an integral condition of membership and safety and security stewardship. Some of the more widely used methodologies include the following.

- The National Association of Chemical Distributors (NACD) revised its Responsible Distribution Process (RDP) in April 2002 to mandate chemical security measures that address potential vulnerabilities within chemical distribution, including site and transportation security and end-use customers. Implementation and third-party verification of RDP is a condition of membership for companies belonging to NACD. RDP's security measures also require Security Vulnerability Assessments (SVAs) to be conducted with onsite, third-party verification.
- The American Petroleum Institute (API)/National Petrochemical and Refiners Association (NPRA), as part of its Facility Security Program, developed the API/NPRA methodology. This comprehensive facility SVA methodology focuses primarily on refineries and petrochemical manufacturers.
- The Chlorine Institute has developed guidance documents regarding the development of security plans by those facilities that handle chlorine rail tank cars when not under the control of a railroad. The guidance calls for an SVA and contains 36 baseline security actions with implementation recommendations and additional security actions for higher alert levels.
- The American Chemistry Council's Responsible Care Security Code also requires facilities to conduct an SVA. A facility can use the Vulnerability Assessment Methodology for Chemical Facilities developed by Sandia National Labs, the Center for Chemical Process Safety (CCPS) SVA methodology, or any other methodology determined certified by the CCPS.
- The Synthetic Organic Chemical Manufacturers Association (SOCMA) developed a computer-based tool, recognized by CCPS as meeting the SVA criteria, that is available, for free, to a wide range of facilities in the Chemical Sector. The SOCMA SVA can be used to help facilities analyze potential vulnerabilities and consider where to most effectively implement enhanced security measures.
- The Agribusiness Security Working Group – comprising the Agricultural Retailers Association, CropLife America, and the Fertilizer Institute – has produced a web-based tool to assist agribusiness retailers in conducting an SVA on their retail facility and their transportation practices.
- The National Paint and Coatings Association recently amended its Coatings Care Program to include a Coatings Care Security Code to address critical areas of site security, transportation, distribution, and cyber security with appropriate management practices and guidelines.

Security Guidance Documents: Several of the individual members of the Chemical Sector Coordinating Council, under the National Infrastructure Protection Plan framework, have developed security guidance documents specific to the sub-sector they represent. Examples include the following:

- The Institute of Makers of Explosives has published explosive industry's best practices standards. Their Safety Library Publication 27 (SLP-27) covers security in the manufacture, transportation, storage, and use of commercial explosives.

SLP-27 also addresses security plans with recommendations tiered to different threat levels.

- Crop Life America sponsors the American Agronomic Stewardship Alliance (AASA), a program designed to inspect and credit more than 6,200 agricultural chemical facilities. The AASA helps to ensure third-party verification at retail sites and to certify that site security plans are developed and implemented.
- ACC, the Chlorine Institute, and SOCMA collaborated on the "Site Security Guidelines for the U.S. Chemical Industry," available for all chemical facilities as a condition of membership and safety and security stewardship.

Public-Private Sector Security Partnerships

Under the National Infrastructure Protection Plan (NIPP), each sector has developed a Sector-Specific Plan, or SSP, which details how the NIPP risk analysis and risk management framework and information sharing network will be tailored and implemented to meet the needs of the sector. The Chemical SSP, released in May of this year, is an excellent example of the public/private partnership DHS has fostered across various levels of government and industry to improve security at chemical facilities around the country. The SSP establishes goals, objectives, and metrics that address a full spectrum of sector collaboration, information sharing, risk analysis, protection, and incident management activities. The chemical sector continues to set a strong example in implementing cooperative strategies that cost-effectively use government and industry resources to help ensure the security of high-risk facilities, systems, and networks.

Through the NIPP process, DHS established solid working relationships with a wide variety of public- and private-sector partners that make up the chemical sector. This partnership provides an effective channel for increased information sharing, risk assessment, collaborative security planning, security-related research and development, best-practices exchanges, and preparations for incident management. The Chemical Sector Coordinating Council (SCC) was formed in 2004 and currently consists of 18 trade associations, with the Chair and Vice Chair positions held by industry operators/owners. The corresponding Government Coordinating Council is comprised of several Federal departments: DHS; as well as the Departments of Commerce, Defense, and Transportation; the Environmental Protection Agency; and the Office of the Director of National Intelligence.

Voluntary Security Collaboration with DHS

The Chemical SSP describes many of the programs through which the Chemical Sector is voluntarily cooperating with DHS to protect and ensure the resiliency of its facilities and manufacturing capacity, as well as the safety of surrounding communities. These programs have also focused on collaborative planning between facility security personnel and federal, state, and local law-enforcement officials to help ensure an integrated "inside-and-outside-the-fence" approach to security.

Specific examples of these voluntary efforts include the following:

Comprehensive Review (CR) Program. This program brings together a federal interagency team, facility owner/operators, industry representatives, and community law-enforcement and emergency-service organizations in a collaborative planning environment. The CR is a structured, collaborative effort among federal government agencies, including DHS components such as the US Coast Guard and the Federal Emergency Management Agency, as well as the Federal Bureau of Investigation; state and local law-enforcement and emergency-management organizations; private-sector owner/operators of critical infrastructure/key resource facilities; and industry representatives. The purpose is to explore vulnerability to a potential terrorist attack, the consequences of such an attack, and the integrated capabilities needed to prevent, mitigate, and respond should such an event occur. The results of the CR are briefed to decision-makers of the site, state and local law-enforcement, and emergency-management organizations at the conclusion of the onsite review week. Gaps and potential enhancements in security and response capabilities are provided to applicable participating organizations for consideration.

The first Chemical Sector CR was conducted in Detroit in February 2006. By August 2007, CRs will have been completed in five additional regions: Chicago, Houston, Los Angeles, Northern New Jersey, and the Lower Delaware River. CRs have identified many improvements – many of them low- or no-cost – that can be implemented by Critical Infrastructure/Key Resources (CI/KR) owners/operators, as well as longer-term strategies and potential improvements that can be implemented with a mix of government and private sector resources.

Buffer Zone Protection Program (BZPP). This program is a targeted grant program designed to assist local law enforcement in enhancing CI/KR protection across the country. For FY 2004/2005, 248 BZPP reports for chemical facilities were submitted to DHS, which are eligible for a total of $12,600,000 in federal grant funding against identified state or local capabilities gaps. For FY 2006, 46 chemical facilities were part of the BZPP, eligible for a total of $10,316,000. For FY 2007, a total of 100 chemical sites are eligible for BZPP funding totaling $19,865,000. To date, 394 chemical facilities have been eligible for a total of $42,781,000 under BZPP. Additionally, in FY 2006, DHS launched a focused $25 million Chemical Sector BZPP to enhance state and local jurisdictions' ability to protect and secure identified chemical facilities in high-risk regions across the country. The Chemical BZPP program is a sector-specific effort designed to be a companion to the Chemical Sector CR initiative.

Chemical Security Awareness Training Program. This program features an online chemical facility security tool for use by all chemical facility employees, not just security officers. This tool is scheduled to be released by the Chemical SSA to the chemical sector in the Fall of 2007.

Vehicle-Borne Improvised Explosive Device Training Program. This program is under development by the Chemical SSA and the DHS Office of Bombing Prevention to provide a course for chemical facility security officers responsible for searching vehicles at chemical plants.

Sector Exercises. Various state-level chemical coordinating councils, in concert with the local first responders and DHS, are conducting tabletop exercises to ensure a coordinated and well-orchestrated response to an event at a chemical facility. Additionally, the Chemical Sector participates as a whole in several national-level exercise events each year. The Chemical Sector

was a participant in the TOPOFF 3 national exercise, from the corporate level to the individual facility level. The sector also participated in the Department of Defense-sponsored exercise "Ardent Sentry" in May 2007, as well as the Continuity of Operations exercise called "Pinnacle" in May 2007. In each exercise, private sector entities and their government counterparts reviewed and tested communication paths and incident management plans and protocols. The Sector is currently planning its participation in the TOPOFF 4 exercise to be conducted in October of this year and is a featured thread in the upcoming Cyber Storm II exercise, which will take place in March 2008.

Chemical Security Summit. In June, DHS and the SCC co-sponsored the 2007 Chemical Sector Security Summit. The event was attended by 350 members of the Chemical Sector. Topics discussed included the implementation of the new CFATS, secure distribution of chemicals, and security-awareness training. Planning is under way for a similar event in 2008.

Homeland Security Threat and Risk Analysis Center (HITRAC). HITRAC has dramatically increased its outreach to the sector during the past two years, providing timely sector assessments, indications and warnings products, and security-related briefings. HITRAC has also worked collaboratively with the private sector to address the timeliness and content of the threat information at the classified and unclassified levels. The last classified brief was in March 2007, and the next one is scheduled for September 2007. In addition, HITRAC provides scheduled bi-weekly unclassified briefings by teleconference on threat information based on private-sector reporting, as well as law enforcement and other sources.

Homeland Security Information Network (HSIN). HSIN is providing an increasing amount of timely information to users in a secure, online format. Recent information that we have posted on HSIN includes information on the July 2007 United Kingdom bombings, reports on recent incidents in Iraq involving chlorine, Quarterly Suspicious Activity Reports, and 2007 pre-season hurricane impacts analysis.

Chemical Security Regulations

As you are all well aware, the FY 2007 Homeland Security Appropriations Act directed DHS to develop and implement a regulatory framework for high-risk chemical facilities. Section 550 of the Act authorizes DHS to require high-risk chemical facilities to complete vulnerability assessments, develop site security plans, and implement protective measures necessary to meet DHS-defined performance standards. The Act gave DHS six months from the date the President signed the Bill, or until early April 2007, to promulgate interim final regulations implementing this authority. DHS published the interim final regulations, the CFATS, on April 9, 2007.

The following core principles guided the development of this regulatory structure:

1) Consultation with industry experts, academic specialists, engineering associations, and non-government organizations to ensure that our rule would be workable while accomplishing our security goals. By working closely with public experts, such as New Jersey State officials and the New Jersey Chemical Council, we believe that we have effectively leveraged vital knowledge and insight to make our regulation better.

2) Tiering. Not all facilities present the same level of risk and that the most scrutiny should be focused on those that, if attacked, could endanger the greatest number of lives, have the greatest economic impact, or present other very significant risks. Low-risk facilities are not a part of this framework.

3) Reasonable, clear, and equitable performance standards for facility security. The rule includes enforceable performance standards based on the types and severity of potential risks posed by terrorists and natural disasters, and facilities should have the flexibility to select among appropriate site-specific security measures that will effectively address those risks, complicating terrorist attack planning and operational surveillance in the process.

4) Recognition of the progress many responsible companies have made to date in raising the security bar across the Chemical Sector. Many companies have made significant capital investments in security since 9/11, and we should build upon that progress in implementing the CFATS program.

Stakeholder input – both public and private – was critical to our success in developing the regulatory framework. In December 2006, DHS released an Advanced Notice of Rulemaking containing a draft regulation for public comment. We received more than 1,300 pages of comments from more than 106 separate submitters. We extensively reviewed these comments and considered them in finalizing the regulation.

Within the Interim Final Rule, we included a second public comment period specific to "Appendix A," which details the specific chemicals and their corresponding "Screening Threshold Quantities" that we intend to regulate through the CFATS program. This public comment period closed out on May 9, 2007, and produced more than 4,000 individual comments for our review. We have studied these comments carefully and are closely considering them as we work to finalize the Appendix. We also conducted extensive outreach with some commenters to better understand their specific concerns and issues.

Issues that informed our initial look at which chemicals could be of concern in developing CFATS included quantities released, potential for theft or diversion, potential for sabotage or contamination, and the effect that they would have on national security, government operations, or the economy.

To implement and execute the CFATS regulations, DHS must define the regulated community or determine which facilities are "high risk." To facilitate this, DHS has developed a screening tool called the Chemical Security Assessment Tool (CSAT). The CSAT employs an easy-to-use, online consequence-based Top Screen tool. CSAT builds upon the foundational assessment tool developed by DHS with industry input referred to as the Risk Analysis and Management for Critical Asset Protection, or RAMCAP. Under the regulatory program, those facilities initially designated high-risk must complete the online CSAT SVA, which will factor into a final determination of a facility's risk level for the purposes of the regulatory regime.

Using the results of the CSAT tools, all high-risk facilities will be placed into one of four tiers based on risk. While all high-risk facilities will be required to develop site security plans addressing their vulnerabilities, the security measures needed to meet the performance standards, as well as its inspection cycle and other regulatory requirements, will be based upon a facility's tier level. The higher a facility's risk tier, the more robust the measures they will need to incorporate and the more frequent and rigorous their inspections will be. Inspections will both validate the adequacy of a facility's site security plan, as well as verify the implementation of the measures identified therein.

DHS is using a phased approach in implementing the CFATS regulations, with implementation at the highest-risk facilities beginning in an expedited manner and implementation at lower-risk facilities occurring in a sequential fashion. The following is a summary of our current activities:

- On June 8, the CSAT Top Screen went live, and the Chemical-Technical Vulnerability Information program (CVI) went into effect. On June 11, we reached out to the State Homeland Security Advisors and the Chemical and Oil and Natural Gas Government Coordinating Councils and SCCs to brief them on program implementation. We kicked off Phase 1(a) the week of June 11, making calls to approximately 50 select facilities to inform them of inclusion in the Phase 1(a) program. This outreach was at the corporate level and is expected to result in a collaborative effort to complete the CSAT Top Screen in an expedited fashion for known high-risk facilities.

Follow-up letters are being sent to companies to serve as a "trigger" for the sixty-day Top Screen clock regarding the initial pool of 50 facilities. The facilities will complete an expedited CSAT process with technical assistance from DHS inspectors. The inspectors are also initiating outreach to state and local jurisdictions to begin security discussions and explain the CFATS program in detail. We anticipate approved site security plans and formal site inspections of these facilities in most cases by the end of the calendar year.

Phase 1(b) also began the week of June 11. This phase is being conducted in coordination with Chemical SCC and Oil and Natural Gas SCC to begin the Top Screen process for additional high-risk facilities <u>at industry discretion</u> prior to publication of Appendix A. This phase provides for Registration and completion of the Top Screen, with a Help Desk available and CVI in place. It gives flexibility in schedule and reflects a partnership model focused on major corporations. A quick glance shows that our outreach efforts are working; as of July 13, the following statistics were reported by our CSAT team:

- 6,096 facilities have registered in the CSAT process and are in some phase of Top Screen completion
- 194 have submitted a completed Top Screen

Phase 2 will commence upon publication of Appendix A and will officially start the program for <u>all</u> facilities that hold chemicals of interest and meet stated screening threshold quantities. Facilities will complete Top Screens, receive preliminary tiering decisions, complete SVAs, develop site security plans, and be inspected to the plan, as appropriate per tier.

In terms of tools to assist compliance with the regulations, the Chemical Terrorism Vulnerability Information Procedures Manual and attendant training are available online at www.dhs.gov/chemicalsecurity.

We intend Phases 1(a) and (b) to be a learning time for us, particularly for our inspectors as well as for industry. What we learn will shape further implementation of the program and help us ensure consistency in our approach across the country.

Additionally, and let me stress that this will be of benefit to all partners in the long run, DHS intends to focus a great deal of effort on fostering solid working relationships with state and local officials and first responders in jurisdictions with high-risk facilities. In fact, to effectively meet the risk-based performance elements under CFATS, facilities must demonstrate that they have active, effective working relationships with local officials in the areas of delaying and responding to a potential attack and knowing who does what during an elevated threat situation. The goal is the same as with our voluntary Comprehensive Reviews: that all stakeholders participate in the planning and implementation of protective security measures around high-risk chemical facilities.

In authorizing the CFATS program, Congress provided the Department with the ability to protect sensitive, chemical-facility information in a way that balances the need to protect the information from inappropriate and potentially harmful disclosures with the need to share the information with key stakeholders, particularly state and local officials. To implement this authority, we conducted a review of existing information security vehicles, including the Sensitive Security Information (SSI) designation. Because neither SSI nor any other existing unclassified designation provides the level of protection called for in Section 550, we developed a designation entitled Chemical-terrorism Vulnerability Information (CVI). That said, the Department does not take the creation of a new information protection regime lightly, especially in light of the President's Memorandum for Heads of Executive Departments and Agencies of December 16, 2005, entitled "Guidelines and Requirements in Support of the Information Sharing Environment," and the current efforts to standardize Controlled Unclassified Information. In addition, DHS has partnered with a working group comprising state and local Homeland Security Officers to implement CVI in a way that supports state and local information needs while ensuring the proper level of information protection to keep sensitive information out of the hands of those who may use it against us.

Conclusion

The Federal government is collaborating extensively with the public, including members of environmental groups and the chemical sector, to actively work toward achieving our collective goals under the NIPP and the CFATS regulatory framework. In almost all cases, industry has voluntarily done a tremendous amount to ensure the security and resiliency of its facilities and systems; however, addressing the concern that such efforts have not been universally adequate in all cases for all high-risk chemical facilities, Congress has directed that the new chemical security regulations be developed and that DHS enforce them. I am hopeful that as we take on this new task, we will continue to work as partners with industry and Congress to get the job done. Given the nature of the terrorist adversary that we face, we simply cannot afford an "us-versus-them" stance toward the Chemical Sector. In this light, "we" will work smartly to implement a risk and performance-based approach to regulation and, in parallel fashion, continue

to pursue the voluntary programs that have borne considerable fruit thus far. We look forward to continued cooperation with all of our industry and state and local government partners as we move towards a more secure future.

Thank you for holding this important and timely hearing. I would be happy to take any questions you might have.