DEPARTMENT OF HOMELAND SECURITY

DHS-2006-0073

RIN 1601-AA41

6 CFR Part 27

Chemical Facility Anti-Terrorism Standards

AGENCY: Department of Homeland Security.

ACTION: Interim Final Rule.

SUMMARY: The Department of Homeland Security (DHS or Department) issues this interim final rule (IFR) pursuant to Section 550 of the Homeland Security Appropriations Act of 2007 (Section 550), which provided the Department with authority to promulgate "interim final regulations" for the security of certain chemical facilities in the United States.

This rule establishes risk-based performance standards for the security of our Nation's chemical facilities. It requires covered chemical facilities to prepare Security Vulnerability Assessments (SVAs), which identify facility security vulnerabilities, and to develop and implement Site Security Plans (SSPs), which include measures that satisfy the identified risk-based performance standards. It also allows certain covered chemical facilities, in specified circumstances, to submit Alternate Security Programs (ASPs) in lieu of an SVA, SSP, or both.

The rule contains associated provisions addressing inspections and audits, recordkeeping, and the protection of information that constitutes Chemical-terrorism Vulnerability Information (CVI). Finally, the rule provides the Department with authority to seek compliance through the issuance of Orders, including Orders Assessing

Civil Penalty and Orders for the Cessation of Operations.

EFFECTIVE DATES: This regulation is effective [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], except for Appendix A to part 27. Subsequent notice will announce the effective date of Appendix A to Part 27.

Comment related to the addition of Appendix A to part 27 only will be accepted until [INSERT DATE 30 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER]

ADDRESSES: You may submit comments, identified by docket number 2006-0073, by one of the following methods:

- Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Mail: IP/CSCD/Dennis Deziel, Mail Stop 8100, Department of Homeland Security, Washington, D.C. 20528-8100.

FOR FURTHER INFORMATION CONTACT: Dennis Deziel, Chemical Security Regulatory Task Force, Department of Homeland Security, 703-235-5263.

SUPPLEMENTARY INFORMATION: This interim final rule is organized as follows: Section I explains the public participation provisions and provides a brief discussion of the statutory and regulatory authority and history; Section II summarizes the changes from the Advance Notice of Rulemaking and discusses the revised rule text; Section III summarizes and responds to the comments the Department received in response to the Advance Notice of Rulemaking; and Section IV contains the regulatory analyses for this interim final rule.

Table of Contents

II. Interim Final Rule
- A. Summary of Changes from Advance Notice of Rulemaking
- B. Rule Provisions

III. Discussion of Comments
- A. Applicability of the Rule
  1. Definition of "Chemical Facility or Facility"
  2. Multiple Owners or Operators
  3. Classifying Facilities Based on Hazard Class
  4. Applicability to Specific Chemicals or Quantities of Chemicals
  5. Applicability to Types of Facilities
  6. Statutory Exemptions
- B. Determining Which Facilities Present a High-Level of Security Risk
  1. Use of the Top-Screen Approach
  2. Assessment Methodologies
  3. Risk-Based Tiers
- C. Security Vulnerability Assessments and Site Security Plans
  1. General Comments
  2. Submitting a Site Security Plan
  3. Content of Site Security Plans
  4. Approval of Site Security Plans
  5. Timing
  6. Alternate Security Programs
- D. Risk-Based Performance Standards
  1. General Approach to Performance Standards
  2. Comments about Specific Performance Standards
  3. Variations in Performance Standards for Risk Tiers
  4. Adoption of MTSA Provisions
- E. Background Checks
- F. Inspections and Audits
  1. Inspections
  2. Third-Party Auditors and Inspectors
- G. Recordkeeping
- H. Orders
- I. Adjudications and Appeals
- J. Information Protection: Chemical-terrorism Vulnerability Information (CVI)
  1. General
  2. Disclosure of CVI
  3. Scope of CVI
  4. Relation of CVI to Other Categories of Protected Information and FOIA
  5. Sharing CVI with State and Local Officials, the Public, and Congress
  6. Litigation
  7. Protection of CVI
- K. Preemption
- L. Implementation of the Rule

I. Introduction and Background

A. Public Participation

Interested persons are invited to participate in this rulemaking by submitting written data, views, or arguments on Appendix A of this interim final rule. Comments that will provide the most assistance to DHS in finalizing the Appendix will reference specific chemicals and Screening Threshold Quantities on the list, explain the reason for any recommended change, and include data, information, or authority that support such recommended change.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Comments that include trade secrets, confidential commercial or financial information, Sensitive Security Information (SSI), or Protected Critical Infrastructure Information (PCII) should not be submitted to the public regulatory docket. Please submit such comments separately from other comments on the rule. Comments containing trade secrets, confidential commercial or financial information, Sensitive Security Information (SSI), or Protected Critical Infrastructure Information (PCII) should be appropriately marked as containing such information and submitted by mail to the individual(s) listed in the **FOR FURTHER INFORMATION CONTACT** section.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov. Submitted comments by mail may also be inspected. To inspect comments, please call Dennis Deziel, 703-235-5263, to arrange for an appointment.

B. Statutory Regulatory Authority and History

On October 4, 2006, the President signed the Department of Homeland Security Appropriations Act of 2007 (the Act), which provides the Department of Homeland Security with the authority to regulate the security of high-risk chemical facilities. See Pub. L. 109-295, sec. 550. Section 550 requires the Secretary of Homeland Security to promulgate interim final regulations "establishing risk-based performance standards for security of chemical facilities" by April 4, 2007. Id. Although interim final regulations are usually issued without prior notice and comment (and the Act requires neither), the Department issued an Advance Notice of Rulemaking (Advance Notice) seeking comment on the significant issues and regulatory text. See generally 71 FR 78276 (Dec. 28, 2006).

As discussed more fully in the Advance Notice, before the enactment of Section 550, the Federal government did not have authority to regulate the security of most chemical facilities. The Department has, however, worked closely with industry leaders in pursuit of voluntary enhancement of security at these facilities and provided both technical assistance and grant funding for security. In addition, through the Coast Guard's Maritime Security regulations, the Department has addressed security at certain maritime-related chemical facilities. See 33 CFR Part 105. Recently, the Departments of Homeland Security and Transportation also proposed security regulations for the rail transportation of hazardous chemicals. See 71 FR 76834, 71 FR 76851 (Dec. 21, 2006). Other Federal programs have addressed chemical facility safety, but not security: the Environmental Protection Agency (EPA) regulates chemical process safety through its Risk Management Plan (RMP) program; the Department of Labor's Occupational Safety and Health Administration (OSHA) regulates workplace safety and health at chemical facilities; the Department of Commerce oversees compliance with the Chemical Weapons Convention; and the Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) regulates, through licenses and permits, the purchase, possession, storage, and transportation of explosives.

With the authority under Section 550, the Department can now fill a significant security gap in the country's anti-terrorism efforts. Section 550 specifies that the regulations "shall apply to chemical facilities that, in the discretion of the Secretary, present high levels of security risk." The statute requires that the regulations establish risk-based performance standards; requires Security Vulnerability Assessments and Site Security Plans; allows Alternative Security Programs; mandates audits and inspections to

determine compliance with the regulations; provides for civil penalties for violation of an order issued under the statute; and allows the Secretary to order a facility to cease operations if the facility is not in compliance with the requirements. The statute also gives the Department the authority to protect from inappropriate public disclosure any information developed pursuant to Section 550, "including vulnerability assessments, site security plans, and other security related information, records, and documents."

As discussed in the Advance Notice, by directing the Secretary to issue "interim final regulations," Congress authorized the Secretary to proceed without the traditional notice-and-comment required by the Administrative Procedure Act. See 71 FR 78276, 78277. The Department, however, saw great benefit in soliciting comments on as much of the program as was practicable in the short timeframe permitted under the statute. Accordingly, the Department voluntarily sought comment on a range of regulatory and implementation issues and responds to the comments below.

II. Interim Final Rule

A. Summary of Changes from Advance Notice of Rulemaking

In this interim final rule, the Department has not changed the general, risk-based approach it proposed in the December 28, 2006, Advance Notice. See 71 FR 78276. As discussed in detail below, the Department plans to implement the regulation in phases, starting to work aggressively with chemical facilities presenting the very highest security risks first. The Department adopts a risk-based tiering structure in its regulatory approach, so that the Department's scrutiny of facilities under this regulation increases as the level of risk increases. Even though this approach remains the same, the Department provides further details below on a number of unresolved issues presented in the Advance

Notice. For example, the Department provides further detail on the issues surrounding background checks for those with access to high-risk facilities, and the Department describes its approach on facilities possessing ammonium nitrate.

On several important issues, the Department has reconsidered and modified the position it proposed in the Advance Notice. For example, in response to comments, the Department has restructured its provisions concerning objections, consultations, adjudications, and appeals. As discussed below, the Department's aim is to provide flexibility and assistance for facilities seeking to comply with the regulatory standards. The Department has decided, however, to incorporate a role for a neutral adjudicator where unresolved differences present themselves and result in significant fines or other penalties. In addition, the Department has modified a number of scheduling and timing requirements in response to comments, and the Department further explains its approach on preemption of state and local law after considering the numerous comments on that subject. Although the Department continues to view as important the opportunity for facilities to submit Alternative Security Programs, the Department modified the circumstances in which it will accept Alternative Security Programs.

Finally, the Department will consider the issues surrounding the use of fees in this regulatory program. The Department is contemplating the assessment of different fees, including filing fees, fees for inspections and audits, and fees for the screening of individuals against the Terrorist Screening Database. The Department has not provided for fees in this interim final rule, but may, in the future, propose and seek comment on the issues surrounding fees for this regulatory program.

B. Rule Provisions

This section summarizes the regulatory text changes that the Department has made to this interim final rule. In addition to the summary contained in this section, we have, in many cases, provided a more extensive discussion of the change, and the reason for the change, in the response to comments below. See § III "Discussion of Comments." Finally, to the extent that the Department has made technical corrections or corrected typographical errors, we do not specifically discuss them.

Subpart A

Section 27.100 Purpose

The Department has added a Purpose section to the rule. It states the Department's purpose and intent in issuing this rule and enforcing this regulatory program.

Section 27.105 Definitions

For purposes of clarity, DHS has added several definitions, including "Chemical Security Assessment Tool," "Chemical-terrorism Vulnerability Information," "Deputy Secretary," "Director of the Chemical Security Division" and "Screening Threshold Quantity." The Department has also revised a few definitions, including "Assistant Secretary" and "Under Secretary." The Department revised "Under Secretary" as a result of organizational changes in the Department following the Post-Katrina Emergency Reform Act, which the President signed on October 4, 2006. See Pub. Law 109-295, Title VI. In several places, the Department indicated that the named official, or his designee, has the specified responsibility under the regulation. The Department also revised the definition of "Alternate Security Program," to provide consistency with changes the Department has since made to § 27.235, the Alternate Security Programs

section. The Department expanded upon the definition of "tier," adding that, for purposes of this part, there are four risk-based tiers.

Finally, the Department made clarifying changes to "Chemical Facility," "Covered Chemical Facility," and "Owner." With respect to the definition of "Chemical Facility," the Department removed the circular nature of the definition in the Advance Notice (i.e., a chemical *facility* shall mean any *facility*) (emphasis added) and now provides that a chemical facility "shall mean any establishment that possesses or plans to possess…."

Section 27.120 Designation of a coordinating official; Consultations and technical assistance

The language in revised § 27.120(a) makes clear that the Assistant Secretary will designate a Coordinating Official responsible for ensuring the uniform, impartial, and fair implementation of these regulations. The language in revised § 27.120(b) indicates that the Coordinating Official and his staff shall provide guidance to facilities, and while the Coordinating Official and his staff will be available for consultation and to provide technical assistance, they will be available only to the extent that resources permit.

In § 27.120(c), the Department has provided specific details as to how a facility requests the assistance of the Coordinating Official. In the second sentence of § 27.120(c), the Department provides that requests for consultation or technical guidance do not serve to toll any of the applicable timelines set forth in this part. Accordingly, regardless of whether or when a facility submits a request for consultation or technical guidance, the Department will require the facility to comply with the regulatory requirements, such as completing the Top-Screen, identifying vulnerabilities in the

Security Vulnerability Assessment, and developing and implementing a Site Security Plan.

The Department has added a new provision in § 27.120(d). This provision provides that a covered facility may request a consultation with the Coordinating Official if it modifies its facility, processes, or the types or quantities of materials that it possesses, and believes such changes may impact the covered facility's obligations under this part. The Department added this provision in response to commenters concerned about a facility's ability to "exit" the regulatory program. The Department recognizes that facilities that reduce risk to levels below those levels that the Department deems as that characterized for Tier 4 facilities (i.e., the lowest risk facilities of the "high risk" facilities) or that eliminate certain risks altogether may no longer need to be covered by this regulation. This provision allows the covered facility to request the initiation of the screening process (which determines whether or not the facility is high-risk and therefore whether the facility is or is not included in this regulatory program) prior to the facility's next scheduled CSAT Top-Screen submission pursuant to § 27.210. Through this consultation process, the facility may initiate discussions with the Department and ultimately accelerate the process for determining whether it can "exit" the regulatory program.

Subpart B

Section 27.200 Information regarding security risk for a chemical facility

The Department has added several new provisions to this section. The Department has revised paragraph (b), by incorporating language from proposed

§ 27.200(a) of the Advance Notice and by also adding new provisions. The two sentences in paragraph (b)(1) come from the end of proposed § 27.200(a). Paragraph (b)(1) provides that the Assistant Secretary may seek the information listed in paragraph (a) by contacting chemical facilities individually or by publishing a notice in the **Federal Register**. It also provides that the Assistant Secretary may instruct facilities to complete and submit a Top-Screen through a secure Department Web site or through any other means approved by the Assistant Secretary.

Paragraph (b)(2) is a new provision. It provides that a facility must complete and submit a Top-Screen in accordance with the schedule provided in § 27.210 if it possesses any of the chemicals listed in Appendix A: "DHS Chemicals of Interest" at the corresponding quantities. For a further discussion of Appendix A, see the discussion of Appendix A further below in the Rule Provisions section. The purpose of this provision is to give facilities direction as to whether or not they must complete and submit a Top-Screen.

As noted in the discussion of Appendix A, the presence or amount of a particular chemical is not an indicator of a facility's coverage under this rule. The presence or amount of a chemical in the Appendix is merely a baseline threshold requiring a facility to complete and submit a Top-Screen. (Consistent with § 27.200(b)(1), DHS will retain the ability to notify facilities, through direct notification or **Federal Register** notice, that they need to complete and submit a Top-Screen.) The information that the Department will obtain through the Top-Screen process is only one of several factors that the Department will consider in determining whether a facility is "high-risk" and thus covered by this rule.

Paragraph (b)(3) addresses the requirements for individuals who submit information to the Department through the CSAT system, which includes the Top-Screen process. Paragraph (b)(3) provides that, where the Department requests that a facility complete and submit a Top-Screen, the facility must designate a person to be responsible for the submission of information through the CSAT system. (The CSAT system is comprised of three sequential parts: the Top-Screen, the SVA, and the SSP). The Department provides that any such submitter must be an officer of the corporation or other person designated by an officer of the corporation, and must be domiciled in the United States. The Department had contemplated such requirements in Appendix A to the Advance Notice and now finalizes them here.

Consistent with the explanation in Appendix A to the Advance Notice, the Department notes that a facility may choose to have another individual, in addition to the above-discussed "submitter," involved in the submission of information through the Top-Screen. That other individual is a "provider." A provider would be a qualified individual who is familiar with the facility in question and who completes the information in the CSAT system. The provider, however, would not formally submit information to the Department. The individual responsible for sending information to the Department through the CSAT system (whether Top-Screen, SVA, or SSP) is always the submitter. And as indicated in paragraph (b)(3), the submitter is also responsible for attesting to the accuracy of the submitted information.

Paragraphs (c)(1) and (2) address facilities that the Department deems as "presumptively high risk." Both paragraphs were in the Advance Notice, though they were located in proposed §§ 27.200(b) and (c).

Section 27.205 Determination that a chemical facility "presents a high level of security risk."

The Advance Notice, at the end of § 27.205(a), contained a provision about Departmental notification to facilities of their preliminary placement in a risk-based tier. The Department has moved that language to § 27.220 "Tiering," so that it is located with the related tiering provisions.

In addition, the Department has removed proposed § 27.205(c), along with §§ 27.220(b), and 27.240(c), all of which had contained a mechanism for objections. In the Advance Notice, the Department had provided facilities with the opportunity to object to the following three Departmental actions: determination that a facility "presents a high level of risk," placement in a high-risk tier, and disapproval of a facility's Site Security Plan. The intention behind those provisions was to provide facilities with an informal opportunity to consult with the Department. The Department believes that the rule (including existing provisions from the Advance Notice as well as new provisions in this interim final rule) provides facilities with several opportunities for consultation when they disagree with an initial decision on these matters. Specifically, revised § 27.120(b) provides that the Coordinating Official and his staff shall be available to consult and to provide technical assistance to a facility owner or operator, revised § 27.120(c) provides the details for how a facility should initiate consultations or assistance, and revised § 27.120(d) provides that a covered facility may request a consultation if it modifies its facility, processes, or the types or quantities of materials that it possesses and believes such changes may impact the covered facility's obligations under this part. In addition, §§ 27.240(b) and 27.245(b) provide that a facility shall enter further consultations

following Departmental written notification that a Security Vulnerability Assessment or Site Security Plan is unsatisfactory. Given that the rule already provides consultation opportunities, coupled with the fact that the Department has greatly modified its adjudication and appeal provisions, the Department believes it is unnecessary to retain these objections provisions and has thus removed them from the interim final rule.

Section 27.210 Submissions Schedule

In § 27.210, the Department clarifies the submission schedule for the Top-Screen, Security Vulnerability Assessment, and Site Security Plan. In § 27.210(a) of the Advance Notice, the Department included a sentence indicating that the presumptive time frames were 60 days for the Security Vulnerability Assessment and 120 days for the Site Security Plan. In this interim final rule, the Department has added presumptive timeframes for the submission of the Top-Screen and revised the presumptive timeframes for SVAs and SSPs. See § 27.210(a) and (b). The presumptive timeframes for initial submissions are 60 calendar days for the Top-Screen, 90 calendar days for the SVA, and 120 calendar days for the SSP. The presumptive timeframes for resubmission vary depending on a facility's tier. As a general matter, the Department will require facilities in Tiers 1 and 2 to update their Top-Screen, SVA, and SSP every two years, and facilities in Tiers 3 and 4 to update their Top-Screen, SVA, and SSP every three years.

In addition, the Department added a new paragraph (c), which addresses the Department's authority to modify schedules as necessary. The Department removed § 27.210(c) as it appeared in the Advance Notice, because the provision was unnecessary in light of the new provisions in § 27.120(b) and (c), "Designation of a coordinating official; consultations and technical assistance."

Finally, the Department added a new paragraph (d), which addresses material modifications. In §§ 27.215(c)(3) and § 27.225(b)(3) of the Advance Notice, the Department provided that a covered facility had to notify the Department of material modifications to the SVA or SSP and that the Department would notify the facility within 60 days of whether the Department disapproved the revised SVA or SSP. The Department has re-located a new but similar requirement in § 27.210(d). The regulation now provides that if a covered facility makes material modifications to its operations or site, the covered facility must complete and submit a revised Top-Screen to the Department within 60 days of completion of the material modification. In accordance with the resubmission requirements in § 27.210(b)(2) and (3), the Department will notify the covered facility as to whether the covered facility must submit a revised Security Vulnerability Assessment, Site Security Plan, or both. As a result of this new paragraph (d), the Department removed the provisions that appeared in §§ 27.215(c)(3) and § 27.225(b)(3) of the Advance Notice.

Section 27.215 Security Vulnerability Assessments and Section 27.225 Site Security Plans

The Department has revised several of the corresponding provisions in both § 27.215 and § 27.225. First, the Department has revised the corresponding provisions regarding methodologies. Specifically, the Department has revised the language in § 27.215(b) and added a new paragraph (b) in § 27.225. In both places, the Department explains that, except as provided in § 27.235, a covered facility must submit either the SVA/SSP through the CSAT process or any other methodology or process identified by the Assistant Secretary.

By this change, the Department is making more explicit its intention to use the CSAT process at this time. The CSAT process includes completion of the Top-Screen process and, depending on the results of the Top-Screen process, may also include the development of a Security Vulnerability Assessment and the development of a Site Security Plan. Thus, for facilities that are determined to be high-risk, the CSAT process will consist of three sequential parts (i.e., the Top-Screen, SVA, and SSP). The Department also notes that facilities will have to obtain access to the CSAT system by submitting a user registration request. Section 27.200(b)(1) contains the requirements for individuals (i.e., submitters) who will be submitting information through the CSAT system and attesting to the accuracy of that information.

Second, in paragraph (c) of both sections, the Department provides that a covered facility must submit an SVA or SSP to the Department in accordance with the schedule provided in § 27.210. This captures the requirement that had been located in proposed § 27.240(a)(1) of the Advance Notice.

Third, in paragraph (d) of both sections, the Department revised the update/revision provisions for submitting SVAs and SSPs. In the Advance Notice, the Department indicated that covered facilities must update or revise their SVAs or SSPs based on a schedule set by the Assistant Secretary. Because the Department has established a submission schedule in § 27.210, the Department now includes cross-references in § 27.215(d)(1) and § 27.225(d)(2) to that schedule. As a related matter, in § 27.215(d), the Department moved the general submissions schedule requirement to § 27.215(d)(1), thereby re-locating the provision formerly in §27.215(d)(1) to §27.215(d)(2).

Fourth, the Department has removed the language about material modifications from proposed § 27.215(c)(3) and § 27.225(b)(3). As discussed in the summary of § 27.210, the Department added a new, but similar, provision to § 27.210(d). The new provision now captures the concept contemplated in proposed § 27.215(c)(3) and § 27.225(b)(3).

With respect to changes to § 27.225 only, the Department has added a provision that requires facilities to conduct annual audits of their Site Security Plans. See § 27.225(e). This provision had been implied in the recordkeeping requirement in the Advance Notice (see § 27.255(a)(6)) and is now explicit. DHS made some additional revisions to the corresponding recordkeeping provision, in which DHS more clearly specifies the audit-related records that covered facilities should maintain.

Finally, throughout this document, the Department now uses the term "Security Vulnerability Assessment" (or SVA) instead of the term "Vulnerability Assessment" or (VA), which the Department had used in the Advance Notice. The Department intends no change in meaning with this revision.

Section 27.220 Tiering

The Department has added several paragraphs to this section. Section 27.220(a) addresses the Department's preliminary determination as to a facility's risk-based tier. Paragraph (a) is based on language that had been in the Advance Notice at the end of § 27.205(a). The Department has elaborated on the Preliminary Tiering provision. Notably, the Department has indicated that it shall notify a facility of the Department's preliminary tiering decision. This contrasts with the Advance Notice, which had merely

indicated that the Department may notify a facility of the Department's preliminary tiering decision.

Section 27.220(b) is not a new subsection; rather, it contains the language that was previously located in § 27.220(a). Note that the Department has removed paragraph (b) as proposed in the Advance Notice. Paragraph (b) had contained an objections provision. For a discussion of the Department's decision to remove the objections provisions from this rule (in §§ 27.205(c), 27.220(b), and 27.240(c)), see the summary under § 27.205(c).

Section 27.220(c) is a new subsection. The Department is reiterating, in part, what it provides in the definitions section. The Department will place facilities in one of four risk-based tiers. Tiers will range from Tier 1, which contains the highest-risk covered facilities, to Tier 4, which contains the lowest-risk covered facilities. Finally, the Department separated the sentence located at the end of proposed § 27.220(a) into its own section, § 27.220(d).

Section 27.230 Risk-Based Performance Standards

This section contains the risk-based performance standards that covered facilities must satisfy. The Department has added a sentence to § 27.230(a), noting that the "acceptable layering of measures used to meet the standards will vary by risk-based tier." While all facilities must satisfy the performance standards, the measures sufficient to meet those standards will be more robust for those facilities that present higher levels of risk. In other words, the manner in which the standards are applied will require a higher level of security (and so provide for greater reduction in risk) for those facilities that

present higher levels of risk. The Department will provide details about the application of these standards in guidance.

In addition, for each of the performance standards, the Department has added a short descriptor at the beginning of the subparagraph (e.g., paragraph (a)(1) begins with "Restricted Area Perimeter," paragraph (a)(2) begins with "Securing Site Assets," and so forth).

The Department has also revised some of the language related to specific performance standards. Section 27.230(a)(4) now provides that facilities must select, develop, and implement measures designed 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." This revised language more adequately captures the concept that the Department had intended in the language in paragraph (a)(4) of the Advance Notice and is more complete. Section 27.230(a)(5) now requires facilities to secure and monitor the storage of hazardous materials, in addition to the shipping and receipt of hazardous materials. Section 27.230(a)(8) now contains a broader description of critical process systems. In the Advance Notice, the Department had used the acronym "SCADA" (Supervisory Control and Data Acquisition) to refer to instrumented control systems in general. In this interim final rule, the Department has provided more descriptive terminology to refer to critical process systems. For a further discussion of SCADA, see the Department responses to "Comments on Specific Performance Standards." Section 27.230(a)(12) contains an expanded standard for background checks. For a further discussion of background checks, see the Department response to comments about "Background Checks." Section 27.230(a)(15) now provides that facilities should report

significant security incidents to local law enforcement in addition to the Department. Finally, the Department has removed the paragraph that was paragraph 27.230(a)(19) in the Advance Notice, because that standard was already addressed in paragraph (a)(14).

Section 27.235 Alternative security program

The Department has revised this section to provide more detail about the process for Alternate Security Programs (ASPs). The basic requirement remains the same, in that certain covered facilities may submit ASPs, and the Assistant Secretary may approve those ASPs. See § 27.235(a). To accept an ASP, the Assistant Secretary must find that the program "provides an equivalent level of security to the level of security established by this part." This language, which clarifies the standard for accepting ASPs, comes from the preamble of the Advance Notice and is consistent with the terms of Section 550. See 71 FR 78276, 78285.

In § 27.235(a)(1) - (2), the Department specifies, by tier, which facilities may submit ASPs in lieu of Security Vulnerability Assessments (SVAs) and which facilities may submit ASPs in lieu of Site Security Plans (SSPs). A Tier 4 facility may submit an ASP in lieu of a Security Vulnerability Assessment, Site Security Plan, or both. Tier 1, Tier 2, and Tier 3 facilities may submit an ASP in lieu of a Site Security Plan. Tier 1, Tier 2, and Tier 3 facilities may not submit an ASP in lieu of a Security Vulnerability Assessment. Accordingly, Tier 1, Tier 2, and Tier 3 facilities will have to submit their SVA through the CSAT system.

With respect to Tier 4 facilities, the Department clarifies the following point: Given that the Department notifies a facility of its final placement in a risk-based tier following the Department's review of a covered facility's SVA (see § 27.220(b)), a

facility will not know its final tier placement at the time it might decide to submit an ASP in lieu of a SVA. Because of that, the Department understands that facilities will rely on the Department's preliminary tiering determination made pursuant to § 27.220(a).

There are various reasons underlying the Department's decision not to accept ASPs as SVAs for Tier 1, Tier 2, and Tier 3 facilities. The Department needs a consistent baseline against which to compare risks and vulnerabilities across chemical facilities. (For a further discussion of this issue, see the Department's response to comments in § III(B)(1)). As well, the Chemical Security Assessment Tool (CSAT) system uses an integrated approach to chemical facility security, and by considering SVAs that use the methodology in the CSAT system, the Department can take full advantage of that integrated approach. Furthermore, by using this electronic, integrated CSAT approach, the Department can more efficiently review and assess a greater number SVAs, and that is of importance considering the Department's phased implementation scheme to address the highest risk facilities first.

The Department acknowledges that many facilities have expended substantial resources and incurred significant expense to identify vulnerabilities and to develop security plans. The Department commends facilities for such efforts. The work performed on these efforts is valuable, and DHS is committed to capitalizing on these investments. The information developed in these efforts will be relevant to facilities as they complete the CSAT SVA. Facilities will be able to use the information from existing vulnerability assessments, and in many cases, the practical impact of requiring Tiers 1, 2, and 3 facilities use the CSAT SVA system will be one of formatting, i.e., facilities will have to enter their information from their existing vulnerability assessments

into the format established by the CSAT system. While some additional analytical effort will be required, even where the facility has produced a strong SVA, the effort will be considerably less than that at facilities that are starting without a pre-existing SVA.

In addition, § 27.235(b) provides that the notice requirements for submitting ASPs correspond with the notice requirements (including the approval and disapproval process) for SVAs and SSPs. In other words, if a facility is submitting an ASP in lieu of an SVA, the process in § 27.240 applies, and if a facility is submitting an ASP in lieu of an SSP, the process in § 27.245 applies.

Section 27.240 Review and Approval of Security Vulnerability Assessment and Section 27.245 Review and Approval of Site Security Plans

In this interim final rule, the Department has separated the review and approval of SVAs and SSPs into two separate sections. In the Advance Notice, both sets of requirements were located in § 27.240. In this interim final rule, the provisions related to Security Vulnerability Assessments are located in § 27.240, and the provisions related to Site Security Plans are located in § 27.245.

In addition, the Department made some changes to the corresponding provisions in the two separate sections. In both sections, the Department has removed the language (from proposed § 27.240(a)(1)) about time periods for submitting SVAs and SSPs. The Department has already addressed this issue in §§ 27.215(c)-(d) and §§ 27.225(c)-(d) (by providing that a facility must provide, update, and revise its SVA and SSP consistent with the schedule in § 27.210), so it was unnecessary to also include this language here. Also, in both sections, the Department has added new language about the disapproval of SVAs or SSPs. The Department added a new sentence, which

provides that "[i]f the resubmitted [SVA or SSP] does not satisfy the requirements of [§ 27.215 or § 27.225], the Department will provide the facility with written notification (including a clear explanation of deficiencies in the [SVA or SSP]) of the Department's disapproval of the [SVA or SSP]." See § 27.240(b) and § 27.245(b).

Finally, the Department has added a provision in § 27.245(a)(1)(iii), indicating that the Department issues a Letter of Approval if it approves a facility's Site Security Plan in accordance with § 27.250. While this provision appears elsewhere in the rule (see §27.245(b)), the Department thought it was appropriate to include it here as well.

The Department has removed 27.240(c) as proposed in the Advance Notice. Paragraph (c) had contained an objections provision. For a discussion of the Department's decision to remove the objections provisions from this rule (in §§ 27.205(c), 27.220(b), and 27.240(c)), see the summary under § 27.205(c).

Section 27.250 Inspections and Audits

The Department has added additional provisions to the inspection and audit section. In § 27.250(c), the Department discusses the time and manner requirements for inspections. While the Department will generally provide facilities with 24-hour advance notice of inspections, the Department recognizes two exceptions where an unannounced inspection might occur. The Department included the first exception in the Advance Notice, and the Department has added the second exception in this interim final rule. For a further discussion, see the Discussion of Comments in § III(F) on "Inspections and Audits."

In § 27.250(d), the Department addresses various details related to the inspectors who will conduct inspections and audits. This is a new paragraph that was not in the

Advance Notice. Although Congress has not provided the Department with administrative subpoena authority, this paragraph explains that inspectors will have credentials and may administer oaths and receive affirmations upon consent. It also provides details about the means by which inspectors may gather information and the access that inspectors will have to records. The Department has also added a paragraph (e), which addresses confidentiality. Finally, the guidance paragraph, which had been located in paragraph (d) has been moved to paragraph (f).

Section 27.255 Recordkeeping Requirements

The Department revised various provisions related to recordkeeping. With respect to § 27.255(a)(1), the Department added a few additional record requirements regarding training. In addition to keeping records of the date and location of each training session, time of day and duration of each session, the name and qualifications of the instructor, and a clear, legible list of the attendees including attendees' signatures, the facility must also keep at least one other unique identifier for each attendee receiving training and the results of any evaluation or training. The Department also added a requirement to § 27.255(b), requiring facilities to keep submitted Top-Screens in addition to submitted SVAs and SSPs. In addition, as discussed above in the summary for § 27.225(e), the Department revised the recordkeeping provision related to internal audits. See § 27.255(a)(6).

The Department also added a new paragraph (c), allowing the Department to request that covered facilities make available records kept pursuant to other Federal programs or regulations. The Department would make such requests for records to the extent that any such records were necessary for security purposes. As a result of adding

new paragraph (c), the Department had to re-designate proposed paragraph (c) as paragraph (d).

Subpart C

The Department has substantially revised Subpart C, which contains the provisions for Orders, Adjudications, and Appeals.

Section 27.300 Orders

The Department has restructured the Orders provisions. Whereas the Advance Notice contained four separate sections (see §§ 27.300, 27.305, 27.310, and 27.315), the Department has now consolidated all of the Order provisions into one section, § 27.300. The main substance of the Orders provisions, however, remains the same. Pursuant to § 27.300(a), the Assistant Secretary can issue an Order for any instance of noncompliance. For example, the Assistant Secretary may issue an Order for a facility's refusal to complete a Top-Screen, failure to allow an inspection, or failure to update a Site Security Plan.

Beyond a basic Order, the Assistant Secretary may issue an Order Assessing Civil Penalty, an Order to Cease Operations, or both, where it determines that a facility is in violation of any Order issued pursuant to paragraph (a). See § 27.300(b). Orders Assessing Civil Penalty are for a continual noncompliance, a repeated pattern of noncompliance or egregious instances of noncompliance. Orders to Cease Operations are the most serious Orders that the Assistant Secretary might choose to issue under this regulatory scheme. The Assistant Secretary will use such a measure cautiously and judiciously and will balance the immediate security needs with the possible impact (e.g., economic impact or national security effect) of such an Order on the chemical industry

and the Nation as a whole. As the Department wrote in the Advance Notice, "This authority would be utilized when no other options will achieve the required result." See 71 FR 78276, 78287.

Paragraphs (c) through (f) of § 27.300 address the process and procedures for Orders. Section 27.300(c) lists the information, at a minimum, that the Assistant Secretary must include in an Order and also notes that the Assistant Secretary may establish further procedures for the issuance of Orders. Section 27.300(d) notes that a facility must comply with the terms of the Order by the date specified in the Order. Section 27.300(e) indicates that a facility has the right to seek an adjudication to review the decision of the Assistant Secretary to issue an Order, and § 27.300(f) addresses final agency action.

With respect to the staying of Orders, the Department addresses this issue in the new adjudications sections. Specifically, § 27.310(b)(4) provides that an Order is stayed from the timely filing of a Notice of Application for Review until the Presiding Officer issues an Initial Decision, unless the Secretary lifts the stay due to exigent circumstances pursuant to § 27.310(d). The new adjudications section is discussed in more depth below.

Section 27.305 through 27.340 Adjudications

Most significantly with respect to adjudications, the Department has provided facilities with the opportunity to seek review of specified decisions before a neutral adjudications officer. A facility or other person may seek review of the following Department (i.e., Assistant Secretary) determinations: (1) A finding, pursuant to § 27.230(a)(12)(iv) that an individual is a potential security threat; (2) The disapproval of

a Site Security Plan pursuant to § 27.245(b); or (3) The issuance of an Order pursuant to § 27.300(a) or (b). See § 27.310(a).

The procedures for Applications are found in § 27.310(b). To institute Adjudication Proceedings, the facility or other person ("Applicant") must file a Notice of Application for Review within seven calendar days of notification of the Assistant Secretary's determination. See § 27.310(b)(1)-(2). Then, in an Application for Review, the Applicant must explain his or her position (i.e., explain why the Assistant Secretary's determination should be set aside). The Applicant has 14 calendar days from the date of notification of the Assistant Secretary's determination to file and serve an Application for Review. See § 27.310(b)(5). The Assistant Secretary, through the Office of the General Counsel, shall file and serve a Response within 14 calendar days of the filing and service of the Application for Review. See § 27.310(c). Finally, the Secretary may make certain procedural modifications in exigent circumstances. See § 27.310(d).

A Presiding Officer is the neutral adjudications officer who handles these proceedings. The Secretary shall appoint a Presiding Officer, consistent with the requirements in § 27.315. A Presiding Officer shall immediately consider whether a summary adjudication of an Application for Review is appropriate, and if the Presiding Officer finds that there is no genuine issue of material fact and that one party or the other is entitled to decision as a matter of law, then the record shall be closed and the Presiding Officer shall issue an Initial Decision on the Application for Review. See § 27.330(b). Such summary decisions are governed by the procedures in § 27.330.

Where there is no summary decision, the Presiding Officer may conduct a hearing using the procedures specified in § 27.335. The Presiding Officer shall close and certify

the record upon the completion of one of the following: a summary judgment proceeding, a hearing, the submission of post-hearing briefs, or the conclusion of oral arguments. See § 27.340(a). Based on the certified record, the Presiding Officer shall issue an Initial Decision, and the decision shall be subject to appeal pursuant to § 27.345.

In addition to the sections mentioned above, there are a few other sections that address provisions related to adjudications. Section 27.320 specifies the prohibition on *ex parte* communications during Proceedings. And § 27.325 provides that the Assistant Secretary bears the initial burden of proving the facts necessary to support the challenged administrative action at every proceeding instituted under this subpart.

Finally, as related to the Appeals section below, a Presiding Officer's Initial Decision is stayed from the timely filing of a Notice of Appeal until the Under Secretary issues a Final Decision, unless the Under Secretary lifts the stay due to exigent circumstances. See § 27.345(b)(4).

Section 27.345 Appeals

The interim final rule contains a revised appeals section. There are several differences. First, a facility or other person may appeal the Initial Decision of the Presiding Officer made pursuant to § 27.340(b). This differs from the Advance Notice, in which a facility could appeal a Departmental final determination regarding disapproval of a Site Security Plan and the Departmental issuance of an Order. See § 27.320 in the Advance Notice. Second, the Advance Notice provided that the Under Secretary would make decisions for most categories of appeals, and the Deputy Secretary would make decisions for one category of appeal. This interim final rule provides that all appeals go to the Under Secretary or his designee acting as a neutral appeals officer. Third, as is

discussed in more depth below, the procedures for an appeal have changed.

The Assistant Secretary, a facility, or other person ("Appellant") may institute an Appeal by filing a Notice of Appeal within seven calendar days of notification of the Presiding Officer's Initial Decision. See § 27.345(b)(1)-(3). The Appellant shall then file and serve a Brief within 28 calendar days of the notification of the Presiding Officer's Initial Decision. See § 27.345(b)(5). The Appellee shall file and serve its Opposition Brief within 28 days of the filing of Appellant's Brief. See § 27.345(b)(6). The Under Secretary shall issue a Final Decision and serve it on the parties. A Final Decision by the Under Secretary constitutes final agency action. See § 27.345(f).

In addition to the provisions mentioned above, the Department notes the following: Pursuant to § 27.345(b), the Under Secretary may provide for an expedited appeal; pursuant to § 27.345(c), *ex parte* communications are prohibited; and pursuant to § 27.345(c), a facility or other person may elect to have the Under Secretary participate in any mediation or other resolution process by expressly waiving, in writing, any argument that such participation has compromised the Appeals process. In addition, pursuant to § 27.345(g), the Secretary may establish procedures for the conduct of appeals.

Subpart D

Section 27.400 Chemical-terrorism vulnerability information

The Department has made numerous clarifying changes to the chemical-terrorism vulnerability information (CVI) section. Some of these changes corrected typographical errors, while several others clarified existing provisions. With respect to a minor change, note that, in § 27.400 of the Advance Notice, the Department referred to CVI as "Chemical-terrorism Security and Vulnerability Information" and in this interim final

rule, the Department now refers to CVI as "Chemical-terrorism Vulnerability Information." The Department intends no change in meaning with this revision.

The Department has highlighted below the more substantive changes to § 27.400. With respect to paragraph (c), the Department has removed paragraph (c)(2), because that concept is already covered in paragraph (e)(1)(v). In paragraph (d)(1), the Department provides that covered persons must protect all CVI in their possession or control, including electronic data. In paragraph (e)(1), the Department added language providing that a person who might have a "need to know" includes "state or local officials, law enforcement officials, and first responders." In paragraph (e)(1)(ii), the Department clarified that a person in training will only have access to CVI that he needs as part of his training, and in paragraph (e)(1)(iv), the Department clarified that a the person in a fiduciary relationship with a covered person who is representing or providing advice to that covered person will also have a need to know CVI. In paragraph (e)(2)(iii), the Department provides that it may require non-Federal persons seeking access to CVI to complete a non-disclosure agreement before such access is granted. In paragraph (f)(3), the Department shortened the distribution limitation statement and added a new sentence at the end, which provides: "[i]n any administrative or judicial proceedings, this information shall be treated as classified information in accordance with 6 CFR §§ 27.400(h) and (i)." And in paragraphs (h)(1), (i)(1), and (i)(2), the Department made it clear that these sections apply to the disclosure of CVI in the context of administrative or judicial enforcement proceedings of section 550 only, not any other kind of enforcement proceeding. Similarly, in paragraph (i)(7)(iii), the Department made it clear that this

section applies only to judicial enforcement proceedings and not any other judicial proceeding.

Section 27.405 Review and preemption of State laws and regulations

The Department has made several changes to § 27.405, including various regulatory text changes. Among those changes, the Department has added paragraph (a)(1). The Department wishes to avoid any unintended consequences in the program's interaction with other Federal requirements. For this reason, § 27.405(a)(1) provides that "[n]othing in this regulation is intended to displace other federal requirements administered by the Environmental Protection Agency, U.S. Department of Justice, U.S. Department of Labor, U.S. Department of Transportation, or other federal agencies." For a further discussion of these changes and preemption in general, see the section below entitled "Executive Order: 13132: Federalism."

Proposed Appendix A: DHS Chemicals of Interest

In the Advance Notice, the Department sought comment on appropriate sources of information or methodologies for evaluating and categorizing chemical facilities." See 71 FR 78276, 78282. The Department responds to those comments below in the "Discussion of Comments." In this interim final rule, the Department has decided to evaluate chemical facility risks by, in part, classifying facilities by particular chemicals. In proposed Appendix A, the Department has included a list of "DHS Chemicals of Interest" along with Screening Threshold Quantities, or STQs, for each chemical. The Department has established STQs to trigger preliminary screening requirements. The STQ is not the threshold quantity for establishing whether a given facility is a high-risk facility, but only sets a threshold to require a facility to complete and submit a CSAT

Top-Screen. As noted in the "Public Participation" section above, the Department is accepting public comment on proposed Appendix A for 30 days. Following the close of the comment period, the Department will review the comments and publish a final Appendix A. The requirements related to Appendix A, which are found in §§ 27.200(b)(2) and 27.210, will become operative on the date that the Department publishes a final Appendix A.

Pursuant to § 27.200(b)(2), if a facility possesses any chemicals identified in Appendix A at the corresponding quantities, the facility must complete and submit a Top-Screen. Consistent with the submission requirements in § 27.210(a)(1), the facility must complete the Top-Screen within 60 calendar days of the effective date of a final Appendix A or within 60 calendar days of coming into possession of any such chemical at the corresponding quantity. (As indicated in the regulatory text, this submission requirement is not operative until the Department publishes a final Appendix A.) Note that this provision does not affect the Department's ability to contact facilities independently of this list. Pursuant to § 27.200(b)(1), DHS may notify facilities, on an individual basis or through an additional **Federal Register** notice, that they need to complete and submit the Top-Screen. The Department notes that, where a facility has a question as to whether it should complete a Top-Screen, the facility can contact the Department and seek a consultation pursuant to § 27.120.

The Department reiterates that the presence or amount of a particular chemical listed in Appendix A is not the sole factor in determining whether a facility presents a high-level of security risk and is not an indicator of a facility's coverage under this rule. The DHS Chemicals of Interest list merely directs certain facilities to complete and

submit the Top-Screen. This list serves as a tool to aid the Department in gathering information needed to administer the program under Section 550. In order for the Department to assess compliance by particular chemical facilities with the regulation (see Section 550(e)), the Department must first obtain information to determine whether the particular chemical facilities qualify for coverage under Section 550. The list set out in Appendix A serves as a procedural tool designed to aid the Department in determining which facilities must comply with the substantive standards. Only after the Department gathers additional information through the Top-Screen process will the Department make a determination as to whether a facility presents a high risk and therefore must comply with the regulatory requirements to ensure adequate security. Under Section 550, the Department has the authority to use its best judgment and all available information in determining whether a facility presents a high level of security risk.

In developing the "DHS Chemicals of Interest" list, the Department has looked to existing sources of information and has then drawn on many of those sources of information, including some of the sources that commenters suggested. Those sources include the following: (1) The chemicals contained on the EPA's RMP list. Pursuant to the Clean Air Act (42 U.S.C. § 7401, et. seq.), which provides that the EPA shall promulgate a list of substances that "in the case of accidental release, are known to cause or may reasonably be anticipated to cause death, injury, or serious adverse effects to human health or the environment (see 42 U.S.C. 7412(r)(3)), the EPA promulgated two lists. Table 1 is titled "List of Regulated Toxic Substances and Threshold Quantities for Accidental Release Prevention," and Table 3 is titled "List of Regulated Flammable Substances and Threshold Quantities for Accidental Release Prevention" (see 40 CFR

§ 68.130); (2) The chemicals from the Chemical Weapons Convention (CWC). Section 6701, et. seq. of Title 22 of the United States Code implements the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction. The CWC covers three lists, or "schedules" of chemicals. Schedule 1 chemicals are provided in Supplement No. 1 to 15 CFR Part 712, Schedule 2 chemicals are provided in Supplement No. 2 to 15 CFR Part 713, and Schedule 3 chemicals are provided in Supplement No. 3 to 15 CFR Part 714; and (3) Hazardous materials, including gases poisonous by inhalation (PIH) and explosive materials, which the Department of Transportation regulates. See 49 CFR § 173.115(c), 49 CFR § 173.50(b), and 49 CFR § 172.101. The Department has also considered other categories of chemicals, such as chemicals that can be used as precursors for Improvised Explosive Devices (IEDs) and certain water-reactive materials that produce toxic gases.

The Department makes a few points with respect to the list in Appendix A. First, DHS is not using any existing list (e.g., the EPA RMP list) as its sole source, and DHS is not classifying all facilities on a list in one particular way (i.e., classifying all RMP facilities as high-risk). By using multiple sources at this initial phase, DHS believes it is obtaining a more complete picture of the universe of facilities that may qualify as high-risk. Second, in identifying the types and STQs of chemicals for Appendix A, the Department has sought to be sufficiently inclusive of chemicals and quantities that might present a high level of risk under the statute without being overly inclusive and therefore capturing facilities which are unlikely to present a high level of risk.

In addition to drawing on information from existing sources, the Department has identified chemicals by considering three security issues. These three security issues, which are explained below, address multiple risk areas.

1. *Release* – DHS believes that certain quantities of toxic, flammable, or explosive chemicals or materials, if released from a facility, have the potential for significant adverse consequences for human life or health.

2. *Theft or Diversion* – DHS believes that certain chemicals or materials, if stolen or diverted, have the potential to be used as weapons or easily converted into weapons using simple chemistry, equipment or techniques in order to create significant adverse consequences for human life or health.

3. *Sabotage or Contamination* – DHS believes that certain chemicals or materials, if mixed with readily-available materials, have the potential to create significant adverse consequences for human life or health.

In proposed Appendix A, the Department lists the DHS Chemicals of Interest and identifies a Standard Threshold Quantity (STQ) for each chemical. To clearly identify each chemical, the Department includes the Chemical Abstract Service (CAS) number for each chemical. These chemicals listed in proposed Appendix A fall into the three categories identified above: chemicals with a release hazard, chemicals with a theft or diversion hazard, and chemicals with a sabotage or contamination hazard.

The Department acknowledges that there are two additional security issues that it is considering at this time, although it is not including any such chemicals that would trigger a Top-Screen submission. They include the following two issues:

1. *Critical Relationship to Government Mission* -- DHS believes that the loss of certain chemicals, materials, or facilities could create significant adverse consequences for national security or the ability of the government to deliver essential services.

2. *Critical Relationship to National Economy* – DHS believes that the loss of certain chemicals, materials or facilities could create significant adverse consequences for the national or regional economy.

The Department is continuing to assess currently-available information about these chemicals critical to government mission and the national economy. The Department will use the information it collects through the Top-Screen process, as well as currently-available information, as a means of identifying facilities responsible for economically critical and mission-critical chemicals.

III. Discussion of Comments

In the Advance Notice, DHS sought comment on proposed text for the interim final rule as well as on various implementation and policy issues concerning the chemical security program. DHS received a total of 106 public comments totaling more than 1,300 pages, including comments from thirty-two trade associations, thirty companies, thirteen private citizens, ten state agencies and associations, seven advocacy and safety groups, eight U.S. Representatives, five U.S. Senators, four unions, one Local Emergency Planning Committee, one professional association, one international standards committee, and the U.S. Small Business Administration.

Commenters generally applauded this effort from the Department and commended the general approach that the Department is taking. However, commenters

also raised some specific concerns. In the sections below, DHS provides a topical summary of the comments and responses to those comments.

A. Applicability of the Rule

1. Definition of "Chemical Facility or Facility"

The Advance Notice defined "Chemical Facility or facility" to mean "any facility that possesses or plans to possess, at any relevant point in time, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criterion identified by the Department. . . ." See proposed § 27.100.

Comment: While a few industry and State agency commenters supported this definition, commenters generally thought that the proposed definition was broad. In particular, several industry commenters, an industry association, a labor union, and a State agency thought the proposed definition was overly broad and consequently did not inform facilities about whether they would be regulated. They noted that the definition did not name the regulated chemical substances or the threshold quantities. One commenter argued that DHS's failure to release to the public its proposed list of "potentially dangerous chemicals" and threshold amounts for those chemicals denies the public the opportunity to comment on key provisions of the rule that depend on whether the facility possess specified quantities of chemicals determined by DHS to be potentially dangerous. The commenter explained that it is difficult to comment on that aspect of the rule without knowing what the chemicals and thresholds are. An industry group cautioned that threshold quantities should be set high enough that retail establishments are not covered merely because they stock commercially acceptable quantities of commonly used chemicals. A few industry commenters and a member of Congress

added that the definition of chemical facility should include the concepts of national security and economic criticality.

Several industry commenters supported the use of EPA's Risk Management Plan (RMP) program to help identify the initial group of regulated facilities. Commenters supported use of the RMP list of toxic substances as a basis for selecting chemical facilities. Likewise, one association felt that DHS should link its definition of chemical facility to those facilities covered by EPA's RMP, because it is a clear and defined list. The industry commenters noted, however, that not all RMP facilities should be considered high-risk. One commenter pointed out that RMP does not take into account facilities that may cause substantial impacts from multiple tanks. A few commenters also recommended that DHS should consider facilities in EPA's Toxic Release Inventory program or facilities that handle DOT hazardous materials.

One commenter emphasized that the rule could focus on toxic gases at RMP threshold quantities, but warned that the RMP program has a different purpose. The commenter indicated that worst-case scenarios under RMP may be based on unrealistic assumptions. Another commenter indicated that DHS should consider certain substances from the Chemical Weapons Convention list when assessing overall risk. Finally, some industry commenters objected to the phrase "possesses or plans to possess," because the term implies legal title or ownership rather than simple presence at the facility.

Response: Aside from the minor modification noted above, DHS is retaining the definition of chemical facility that it proposed in the Advance Notice. And while DHS is not defining "chemical facility" by listing specific chemicals, DHS is making available, with the issuance of this rule, a list of those chemicals and Screening Threshold

Quantities (STQs) that it proposes to use to determine whether to further assess whether a chemical facility presents a high risk. Specifically, if a facility possesses any of the chemicals, at the corresponding quantities, in Appendix A (when finalized), the facility must complete and submit a Top-Screen within 60 calendar days. See § 27.200(b)(2) and § 27.210(a). The Department will continue to contact facilities individually and through additional **Federal Register** notices, as necessary. See § 27.200(b)(1). To the extent the Department notifies facilities through an additional **Federal Register** notice, the Department will engage in outreach activities with the chemical sector.

Finally, in response to specific comments above, the Department makes two additional points. The Department has retained the phrase "possesses or plans to possess." DHS believes that phrase adequately captures the Department's intent. The plain meaning of those terms is not limited to ownership. Also, with respect to the commenter who cautioned that any types of threshold quantities should be high enough so that DHS does not cover all retail establishments that stock commercially acceptable quantities of commonly used chemicals, DHS notes that it is aware of that issue. While DHS believes these STQs are set at levels that normally will not cover such retail establishments, DHS believes that, if a retail establishment does exceed any of these STQs, the retail establishment will have to complete the Top-Screen.

2. Multiple Owners and Operators

The second half of the definition of "Chemical Facility or facility" provides that the terms "shall also refer to the owner or operator of the chemical facility. Where multiple owners and/or operators function within a common infrastructure or within a

single fenced area, the Assistant Secretary may determine that such owners and operators constitute multiple chemical facilities depending on the circumstances." See § 27.105.

Comment: Comments were varied on the issue of multiple owners and operators. One industry commenter suggested that DHS should combine adjacent facilities under common ownership into a single facility, and other industry commenters thought that DHS should define certain adjacent facilities as less than the entire property. One industry commenter thought that DHS should allow facilities with multiple owners or operators to agree among themselves how to meet the requirements of this rule. A trade association noted that some large chemical facilities have third-party warehouses and leasing agreements and that the owners of the chemical facility should be responsible for security.

Response: DHS believes that it will generally be fairly straightforward for facilities to define their boundaries and identify the party (at their facility) that is responsible for compliance with the regulation. However, DHS acknowledges that, in some circumstances, the issue might be more complex. The Department will address these situations on a case-by-case basis. Both owners and operators of facilities, however, bear responsibility under the regulations for implementing measures that meet the regulatory standards.

3. Classifying Facilities Based on Hazard Class

Comment: In the preamble to the Advance Notice, DHS requested comment on whether it should use an approach based on hazard class, rather than use an approach where classifications are based on particular chemicals. Responses were mixed.

Several commenters favored the hazard class approach, noting that facilities are familiar with the DOT hazard classes, that the hazard classes may be harmonized with international requirements, and that the number of chemicals (in a non-hazard class approach) might otherwise be very large. Some of the commenters who favored the hazard class approach also noted some caveats to its use. Industry commenters and a State agency warned that the hazard class approach could result in the inclusion of chemicals that do not pose a security risk. Conversely, others noted that the hazard classes may not include chemicals of concern from a terrorism perspective. Commenters noted that other agencies may regulate the hazard classes under other programs. Also, one State agency association pointed out that a combination of chemicals might be more dangerous than any one chemical. One firm suggested that the DHS approach should include both the hazard class approach and the classification of chemicals approach.

A few industry commenters indicated that basing the applicability of the rule on hazard classes would be inappropriate and that they favored a list of security-sensitive chemicals with threshold quantities. One trade association supported the use of lists of particular chemicals, explaining that they thought it would lead to more accurate assessments of likelihood and consequence and therefore risk. They also argued that DHS publish the list in the final rule.

Response: As explained above, DHS is publishing a list of "Chemicals of Interest" in Appendix A to this interim final rule. The list contains specific chemicals and STQs. That list is a baseline screening threshold against which facilities will know whether they need to complete and submit a Top-Screen. While DHS's primary

approach will be through the classification of chemicals, DHS will not preclude the use of the hazard classes for certain purposes in the performance standard guidelines.

4. Applicability to Specific Chemicals or Quantities of Chemicals

Comment: Several commenters discussed specific chemicals and whether or not the regulation should cover facilities that possess those chemicals. Several commenters thought that DHS should not cover anhydrous ammonia or ammonium nitrate, both of which are discussed in more depth below. A local government agency urged DHS to cover facilities that store propane, while other commenters indicated that DHS should not cover flammable fuels such as propane. A few commenters noted that some facilities may have only small amounts of chemicals or may handle them only intermittently. A trade association suggested that DHS should allow such facilities to adjust their level of security to the level of risk. Another commenter urged DHS to consider the nature of batch production facilities, which make a continually changing mix of products using a continually changing, and often unpredictable, mix of ingredients.

With respect to anhydrous ammonia, commenters noted that the chemical is in the EPA RMP list but indicated that it should not be a chemical that DHS regulates. They explained that ammonia refrigeration is used for dairy and food processing facilities and that those facilities do not pose a significant risk to human health, national security, or the economy, because an attack on such a facility would not result in a catastrophic release of ammonia. In addition, the commenters stated that the food industry (which uses anhydrous ammonia for refrigeration) should not have to spend its resources enhancing security for refrigeration systems.

With respect to ammonium nitrate (AN), some industry commenters noted that AN is an important part of the economy in both the explosives and the fertilizer industries. They noted that the threat posed by AN is not that of a direct attack but of theft or diversion for later criminal misuse. While they said that DHS should focus not only on the possibility of a direct attack at facilities with "weaponizable" chemicals, but on facilities with risks of theft or diversion, they suggested that DHS place those facilities (i.e., those with risk of theft or diversion) in lower-risk tiers.

One commenter recommended requirements for chain-of-custody control and suggested that the ATF could assist in enforcement at AN sites with commercial explosives; other commenters favored regulation by DHS, not ATF. Another commenter believed that DHS should work with the U.S. Department of Agriculture and producer groups in deciding whether to regulate an agriculture operator or supplier. An industry commenter noted that the mere presence of AN at a site should not trigger application of DHS's screening process. Two members of Congress argued that the rule should apply to AN manufacturing facilities, but they agreed with DHS and other commenters that DHS should subject AN facilities to regulatory requirements based on the nature of the facility and risk assessment results. The commenters thought that by including AN facilities in the regulatory program, DHS would make it more difficult for terrorists to acquire this product.

Response: The Department's regulatory scheme will cover chemical facilities that present a high risk because they possess or plan to possess chemicals that terrorists may use or target in the furtherance of acts of terrorism. Facilities that possess chemicals that are hazardous and can be used as weapons, such as anhydrous ammonia or ammonium

nitrate, will be regulated if they present a high risk. However, a facility that possesses a chemical substance that does not cause it to present a high risk (taking into account all relevant factors), or possesses an otherwise hazardous chemical in an amount that is below what would cause the facility to present a high risk (again, taking into consideration all relevant factors), will not be regulated.

Accordingly, with this interim final rule, DHS plans to regulate high-risk facilities with ammonium nitrate and anhydrous ammonia using the same risk-based approach under which it plans to regulate all other high-risk facilities. If DHS later decides that any individual chemicals warrant specialized attention in regulatory provisions, DHS will address such chemicals through future rulemakings.

5. Applicability to Types of Facilities

Comment: A few commenters suggested that the rule should not apply to railroad facilities, because such facilities are covered by current and proposed requirements from the Department of Transportation's (DOT) Federal Railroad Administration and Pipeline and Hazardous Materials Safety Administration and DHS's Transportation Security Administration (TSA). Those commenters asserted that railroads should be treated separately from fixed facilities and that the proposed requirements are inappropriate for railroad facilities. One commenter requested exemptions for motor vehicles and rail cars that are "in transit." Another commenter asked DHS to take a system-wide approach and recognize the interdependence of chemical facility and rail security.

Response: Regulating chemicals in the railroad system is a complex issue, and DHS continues to evaluate it. TSA is the lead component within DHS for the security of transportation facilities and has initiated some recent efforts to address rail security,

including Voluntary Agreements with the rail industry and a Notice of Proposed Rulemaking on Rail Transportation Security. See 71 FR 76852 (December 21, 2006). With respect to chemical security, certain aspects of Section 550 and TSA's authorities are concurrent and overlapping. DHS is working, and will continue to work, with its components, including TSA, to determine whether DHS will include railroad facilities in its chemical security program. DHS presently does not plan to screen railroad facilities for inclusion in the Section 550 regulatory program, and therefore DHS will not request that railroads complete the Top-Screen risk assessment methodology. DHS may in the future, however, re-evaluate the coverage of railroads, and would issue a rulemaking to consider the matter.

Comment: Commenters asked about the applicability of the rule to natural gas pipelines and facilities, with some noting that DHS should not regulate pipelines because DOT/PHMSA and DHS/TSA already regulate safety and security of pipelines. Other commenters asked about DHS's plans to address other large facilities, such as mines. One engineer pointed out that mining facilities can be very large and can cover thousands or tens of thousands acres but that the security-sensitive portions of those mines may be very small (e.g., a single tank).

Response: Whether a facility is covered under this regulation is driven by a number of factors, including the specific types and quantities of chemicals at a given facility. Whether the Department will apply the requirements of this regulation to a facility depends, in part, on the chemicals present at that facility. In the case of natural gas pipelines, DHS has no intention at this time of requiring long-haul pipelines to complete the Top-Screen (or prepare Security Vulnerability Assessments and develop

Site Security Plans). But chemical facilities otherwise covered by this regulation and with pipelines within their boundaries must treat those pipelines like any other asset, i.e., include measures in their Site Security Plan addressing the security of those pipelines.

Related to this, DHS makes a clarifying point about facility assets in general. DHS expects that facilities will address all facility assets in their Security Vulnerability Assessments and Site Security Plans, as any given facility asset has the potential to have an effect on the consequence and/or vulnerabilities of the facility. Facility assets include any items or structures (such as buildings, vehicles, laboratories, or test facilities) located on an area owned, operated, or used by the facility. Such assets may exist inside or outside of perimeter structures.

Similarly, the extent of coverage of mines in this regulation will depend in part on the type and amount of chemicals present at any given mine facility. The Department expects that mines will comply with the requirements of § 27.200(b) and complete and submit the Top-Screen as required in that section. With respect to large mines that may only possess a concentrated amount of a given chemical in one discrete location, if the given chemical (and quantity) is one that the Department believes presents a security risk, the Department will expect that the facility will go through the screening process. While the facility may have to develop a Site Security Plan, the SSP would be tailored to the specific circumstances at the mine. The SSP for a large mine with a concentrated amount of one chemical in one location would surely look dramatically different than that of mine company with different circumstances (e.g., a large mine with larger quantities of different types of chemicals spread throughout the mine or a smaller mine with moderate quantities of very hazardous chemicals in several different locations).

6. Statutory Exemptions

Comment: Some commenters asked why § 27.105(b) excluded certain facilities from the rule, and another commenter suggested that the exempted facilities should be reviewed to determine if they would be considered high-risk but for the exemption.

Other commenters suggested additional exemptions. One commenter suggested that the rule should not apply to most facilities that manufacture, sell, or reclaim lead-acid batteries, and another commenter believed DHS should exclude pesticide facilities. Yet another commenter thought that most facilities storing petroleum products, some of which are exempted under proposed § 27.105(b), are not high-risk facilities.

Response: In the authorizing legislation for this regulation, Congress exempted various facilities from this rule. See Section 550(a). DHS has included those exemptions in § 27.110(b) of the rule. The statute provides for the following exemptions: facilities regulated pursuant to the Maritime Transportation Security Act of 2002, Public Law 107-295, as amended; public water systems (as defined by Section 1401 of the Safe Drinking Water Act); water treatment works facilities (as defined by Section 212 of the Federal Water Pollution Control Act); any facilities owned or operated by the Departments of Defense and Energy; and any facilities subject to regulation by the Nuclear Regulatory Commission. The Department has considered the exemptions requested by commenters, and, at this time, the Department does not intend to provide any additional regulatory text exemptions.

Comment: Some industry commenters supported the exemptions in § 27.110, such as the exemption for facilities regulated under the Maritime Transportation Security Act (MTSA). In addition, one association wanted to exclude from the Top-Screen

requirements any facilities covered under MTSA. Other commenters asked for clarifying information about the exemptions.

Response: In the Advance Notice, the Department discussed the applicability of this rule to maritime facilities. See 71 FR 78276, 78290. In this interim final rule, the Department clarifies that it will apply the statutory exemption only to facilities regulated under 33 CFR Part 105, Maritime Facility Security regulations. Part 105 of Title 33 of the Code of Federal Regulations is the only regulation that imposes the security plan requirements of 46 U.S.C. 70103 on maritime facilities.

Comment: A State agency believed that the Nuclear Regulatory Commission (NRC) exemption should apply only to facilities holding an NRC power reactor license and disagreed with the exemptions for public water systems and treatment works.

Response: The Department agrees with the commenter and will apply the statutory exemption to facilities where NRC already imposes significant security requirements and regulates the safety and security of most of the facility, not just a few radioactive sources. For example, a power reactor holding a license under 10 CFR Part 50, a special nuclear material fuel cycle holding a license under 10 CFR Part 70, and facilities licensed under 10 CFR Parts 30 and 40 that have received security orders requiring increased protection, will all be exempt from 6 CFR Part 27. A facility that only possesses small radioactive sources for chemical process control equipment, gauges, and dials, will not be exempt.

B. Determining Which Facilities Present a High-Level of Security Risk

1. Use of the Top-Screen Approach

Comment: In general, many industry associations and chemical companies supported the use of a tiered approach that narrows DHS's focus to high-risk facilities. Several commenters pointed out as a problem the fact that they had been unable to review the details of the approach and associated criteria; several commenters suggested that knowledgeable parties should have an opportunity to review the details. Many of the commenters wanted to make sure that the final group of high-risk facilities was determined based on risk (not just on potential consequence or limited pieces of threat data) and that the number of facilities in this group was small.

Associations differed in their views on how inclusive the Top-Screen process should be—one association wanted DHS to screen out certain low-risk facilities in the first few questions while other associations and a chemical company wanted DHS to make sure that as many facilities as possible submitted Top-Screen data, including some facilities that might not traditionally be considered chemical facilities. Several associations urged DHS not to presumptively classify facilities as high-risk without perfect information; they felt that doing so would go beyond the authority that Congress granted DHS and would not match the intended focus on high-risk facilities. A local agency took the opposite view on that question.

Several commenters provided input on the data that facilities will need to enter into the Top-Screen. One association suggested that DHS allow facilities to enter chemical volumes in ranges and asked that DHS provide guidance on handling mixtures and blends. That association also questioned how facilities should address chemicals that are stored offsite. Another association encouraged DHS to include reactive chemicals

and propane in the Top-Screen. One advocacy group encouraged DHS to incorporate chemical transportation in the rule and the Top-Screen.

Commenters also provided input on how DHS should process the information that it receives through the Top-Screen. One industry association suggested that facilities should be allowed to explain "yes" responses before DHS drives the facility to a full Security Vulnerability Assessment. The association suggested that facilities should not be the ones to estimate consequences, particularly injuries, and that DHS should refine the definition of injuries. The association stated that DHS should have different requirements for facilities that only periodically have certain materials onsite. One association cautioned about using RMP data and advocated for DHS to use conversion factors to make estimates of casualties.

Several commenters were concerned about the questions in the Top-Screen that related to economic impacts. Several associations indicated that DHS should use a sufficiently high threshold for economic impacts that captures the full extent of economic impacts. They noted that a facility should consider all impacts, not just the impacts to one facility. One association commented that most facilities will not be able to provide answers to the questions in the Top-Screen that ask about a facility's market share for given chemicals. That association suggested that DHS re-phrase those questions to support yes/no answers or to allow facilities to use broad ranges.

Several associations commented that the submitting company, not DHS, should determine the most appropriate person to submit data. A number of parties commented on DHS's subsequent use of the data that is collected through the Top-Screen. One

association commented that any information must have demonstrated utility before it is shared with anyone.

As for timing, commenters, including State agencies, requested that DHS provide facilities with the specific timing requirements for completing the Top-Screen. One industry association recommended that DHS use phased-in timing for having facilities complete the Top-Screen. A number of commenters from State agencies and industry associations suggested the need for DHS to provide active, written notification that a facility is not high risk—and for telling facilities that they need to comply with the regulation. One association suggested that DHS provide this notification immediately upon the facility's submission of data.

Finally, a number of company and industry association commenters wanted to make sure that facilities have the opportunity to conduct independent evaluations (or meet with DHS) to verify or deny DHS's initial classification of a facility's risk.

Response: In this regulatory program, DHS will employ a modified version of the Risk Analysis and Management for Critical Asset Protection (RAMCAP) risk assessment methodology known as the Chemical Security Assessment Tool, or CSAT. The RAMCAP Sector Specific Guidance was developed under contract to DHS by the ASME Innovative Technologies Institute (ASME-ITI) and leveraged the knowledge and insight of leading experts from across the industry and Federal Government. The DHS Risk Assessment Methodology is composed of two separate parts. The first part is a screening tool known as the Top-Screen, which is used to perform a preliminary "consequence" analysis. The second part provides the tools to conduct a thorough facility Security Vulnerability Assessment.

DHS is using a standard vulnerability tool, the CSAT system, because it is not practical for DHS to accept a broad spectrum of methodologies. Even where certain "equivalencies" exist between methodologies, the equivalencies can only be extracted and employed in a comparative risk analysis at very great cost and over a very long period of time. In order to effectively manage risk at the national level, the Department must be able to develop and understand the relative risk of different facilities. A comparative risk capability is essential to regulation and can be achieved only through the collection of comparative data. Thus, a standard vulnerability tool is necessary.

The Department has vetted the CSAT system with the engineering profession, the National Laboratories, and academia. The Top-Screen component, as well as the individual algorithms employed in the Top-Screen, have been subject to extensive peer review and have been found acceptable. While the Top-Screen is consequence-specific, DHS uses the Top-Screen only to determine a preliminary tier ranking. DHS bases a facility's final tier ranking upon the complete Security Vulnerability Assessment, as well as the application of threat information – and thus it is risk-based.

Insofar as the range of facilities possessing dangerous or potentially dangerous chemicals is large, there is no good alternative to a fairly broad range of facilities being included in the screening process. DHS anticipates that the vast majority of screened facilities will be found not to have a level of potential consequences that would result in a "high risk" designation. However, the facilities that do achieve that level of consequence are expected to come from a fairly broad swath of the Nation's economy. DHS has no intention of classifying facilities as presumptively high risk until and unless DHS is unable to acquire sufficient data.

The Top-Screen will enable DHS to determine a preliminary tier based on consequence. That ranking will determine the need for (and timeline for) a Security Vulnerability Assessment, and where the Top-Screen indicates the need for a follow-on Security Vulnerability Assessment, DHS will expect that the owner-operator will comply. The Department will require facilities to submit the Top-Screen within the timeframes now specified in § 27.210. The Department notes that the Top-Screen is designed to preclude a large number of "false negatives."

DHS is establishing the entire CSAT system as an on-line suite of tools, which will allow notification of results to the owner or operator. As provided in § 27.205, the Department "shall notify the facility in writing [of a determination that the facility presents a high level of security risk]." While the online feature of the CSAT system will allow rapid results, it will not allow the Department to respond instantaneously, as some commenters requested. Finally, the Top-Screen tool does require the owner-operator to provide certain data similar to an RMP analysis; however, casualty estimates and consequence ranking are performed by DHS using well-vetted formulae.

Regarding economic criticality, DHS recognizes the complexity of estimating potential economic or mission impact stemming from the loss of certain manufacturing (or other) capacity. Accordingly, DHS will focus early efforts on developing a sufficiently clear picture of the chemical industry as a system in order to allow a reasonable analysis of economic and mission criticality, which will be enhanced as the Department moves forward.

2. Assessment Methodologies

Comment: Many commenters provided input on methodologies that DHS should use for determining which facilities present a high level of risk, and several commenters had suggestions as to how DHS should determine which facilities are high-risk. One association asserted that DHS needed to clearly define the "risk of interest" before DHS could determine which methodology to use. One (non-chemical) company suggested that DHS use other Federal programs such as the EPA's Toxics Release Inventory or the Superfund Amendments and Reauthorization Act (SARA) Tier II annual reports to determine high risk facilities. Commenters addressed the suitability of both asset- and scenario-based approaches, with the majority favoring an asset-based approach. Commenters suggested that DHS consider specific methodologies developed by associations, national laboratories, or State and Federal agencies. One association suggested that DHS use other methodologies while RAMCAP continues to develop and mature. State agency commenters warned that the question of which facilities pose a high risk is a community-specific issue.

Many comments were very specific as to how DHS should proceed, and what tools DHS should employ. For example, an engineering firm focused on the need for process-based assessments. A chemical company noted the need for any approved methodology to also consider the criticality of surrounding and supporting infrastructure in a reasonable manner—that is, one that is within the expertise of the facility personnel.

Many commenters also focused on various aspects related to RAMCAP. One commenter asserted that RAMCAP might not adequately identify high-risk facilities. Another commenter asked who owns RAMCAP. Several commenters noted that the RAMCAP approach was not designed to address control system cyber security. Another

commenter felt that DHS provided inadequate detail on the RAMCAP methodology and noted that DHS should define the method before DHS solicits comment. Several commenters also pointed out that RAMCAP's lack of details on vulnerability team composition and experience could be a limitation. Some of RAMCAP's developers took issue with deviations from the original RAMCAP design. Another commenter pointed out the need for DHS to include proper references to the RAMCAP and its genesis.

Also related to RAMCAP, some commenters expressed concern with the details in Appendix B, "Background: Risk Analysis and Management Critical Asset Protection (RAMCAP) Vulnerability Assessment Methodology." In particular, some expressed concern about expectations that the noted threat scenarios would be analyzed as design basis threats. The commenters noted that many of the scenarios require military support to defeat, and that appears to be beyond the capability of a chemical facility to address. Associations noted that scenarios can be useful in a comparative top-screen, but that they should not guide all facility-specific assessments. One company opined that the threats needed to be more realistic before they were used in any assessments.

Finally, one chemical company commented that DHS needs to list in the rule the specific threats that facilities need to address in their SSP. Also, the company indicated that DHS, not individual companies, should determine deaths and injuries.

Response: In the Advance Notice, DHS sought to provide an overview of RAMCAP and the DHS Methodology Assessment in the preamble (see, e.g., pgs 78277-78288) and in Appendix B. As there seemed to be confusion about the nature and purpose of RAMCAP and the DHS Assessment Methodology (or CSAT) and its purpose, DHS provides further explanation here.

The CSAT vulnerability assessment tool, part of the CSAT system owned by DHS, is an asset-based vulnerability assessment tool very similar to the Chemical Sector RAMCAP module. The CSAT system employs a set of defined attack vectors, used to both "produce" consequences (for the measurement of criticality) and to measure vulnerability. These are not "Design Basis" threats and in no way reflect the type of actual threats against which owner-operators will be expected to "defend." They are measurement devices, supporting the DHS need to conduct comparative risk analysis. The CSAT tool does include basic assessments of certain types of cyber systems, and certain features thereof. However, the CSAT tool is not intended to be a full-scope, detailed analysis of all possible areas of vulnerability. It is a measurement tool that will allow general categorization of a facility as vulnerable or not, critical or not, and thus, at risk or not. DHS will undertake detailed evaluations of specific security issues as part of the ongoing relationship between the facility owner-operator and DHS. The assessment tool that DHS uses to conduct comparative risk assessments must be uniform and consistent in order for DHS to use it, and so a "menu" of different methodologies is simply not practical.

Finally, DHS notes that there were several comments from companies, encouraging the Department to adopt or require their own methodology or technique. DHS is unaware of the extent of peer review or scientific evaluation of these other methodologies or techniques. In addition, DHS does not believe it is appropriate to identify a single commercial product or endorse particular commercial products for purposes of complying with this rule.

3. Risk-Based Tiers

In the Advance Notice, the Department asked for comment on the notion of risk-based tiering of high-risk facilities. Specifically, the Department asked how many risk-based tiers should the Department create, what the criteria should be for differentiating among tiers, what the types of risk should be most critical in the tiering, how should performance standards differ among risk-based tiers, what additional levels of regulatory scrutiny should DHS apply to each tier. 71 FR 78276, 78283.

Comment: Most commenters supported the establishment of risk tiers and agreed that three or four tiers would be sufficient. Several comments, including industry commenters, State agencies, and a member of Congress believed that DHS should base tiering on the attractiveness of the facility as a target or the consequences of a terrorist attack, such as adverse impacts on public health and welfare, the potential for mass casualties, and disruption of essential services. The commenter indicated that the creation of tiers would allow facilities to maintain security measures commensurate with risk.

A few commenters suggested that DHS did not provide enough information in the Advance Notice on the number of tiers or on how a tier classification would affect a facility's security requirements. Two industry commenters were concerned that DHS might apply the rule requirements to facilities other than those that pose the highest security risk. Two other commenters believed that the tiering approach is not appropriate for cyber security of control systems. One commenter argued that tiers should include consideration of the transportation of chemicals outside the facility property. Another commenter recommended that DHS should modify the tiers after it receives data from regulated facilities. Another commenter thought that DHS should define "present high

levels of security risk" and "high risk" at the end of the RAMCAP process and not at the discretion of the Secretary.

Commenters suggested that tiers should be objective and transparent and should provide flexibility. One industry commenter pointed out that tiering allows DHS to focus on the most important facilities first and believed that DHS should establish a de minimis tier that sets thresholds below which a facility does not have to complete the Top-Screen tool. Two commenters noted that tiering provides an incentive for facilities to eliminate risk.

Some industry commenters and State and local agencies suggested that facilities in higher risk tiers should have more contact with DHS, and that lower-risk facilities should have fewer security layers implemented over a longer period of time, greater discretion, or fewer inspections. One commenter, however, believed there should be no difference in regulatory scrutiny or performance standards between tiers.

Response: The Department agrees with many of the commenters that the risk-based tiering structure will allow DHS to focus its efforts on the highest risk facilities first. To that end, the Department intends to retain the model proposed in the Advance Notice. See, e.g., 71 FR 78276, 78283. In sum, the Department's framework for risk-based tiering will consist of four risk-based tiers of high-risk facilities, ranging from high (Tier 1) to low (Tier 4). The Department will use a variety of factors in determining which tier facilities will be placed, including information about the public health and safety risk, economic impact, and mission critical aspects of the given chemicals and Threshold Quantities (TQ) of the chemicals. The Department considers the methods for determining these tiers to be sensitive anti-terrorism information that may be protected

from further disclosure. The types and intensity of security measures (necessary to satisfy the risk-based performance standards in the facility's Site Security Plan) will depend on the facility's tier. The Department will mandate the most rigorous levels of protection and regulatory scrutiny for facilities that present the greatest degree of risk. Finally, pursuant to Section 550(a), it is in the discretion of the Secretary to apply regulatory requirements to those facilities that present high levels of security risk; accordingly, the Department believes it is most appropriate for the Secretary to determine which facilities present high-risk (and not, for example, rely solely on output from the CSAT process).

The Department incorporates the concept of "target attractiveness" into its risk equation. Insofar as it is a fairly subjective element, and that it requires considerable analysis to develop, DHS will not incorporate it into the initial tier assignment process. However, insofar as "target attractiveness" is included in the more detailed Security Vulnerability Assessment component of the regulatory process, and insofar as the final determination of tier placement will be based upon the complete analysis of risk, "target attractiveness" will, in fact, be an important element in tier assignment and subsequent risk management efforts.

C. Security Vulnerability Assessments and Site Security Plans

1. General Comments

Comment: One association requested that DHS encourage, but not require, facilities that are not high-risk to conduct vulnerability assessments as a best practice.

Response: The Department has always encouraged the chemical sector to analyze security vulnerabilities and will continue to do so through voluntary sector efforts even if the site has not been designated as high risk under this rule.

Comment: One commenter requested that DHS define "material modifications," as used in §§ 27.215(c)(3) and 27.225(b)(3), or at least provide examples of circumstances or events that rise to the level of "material modifications."

Response: Material modifications can include a whole host of changes, and for that reason, the Department cannot provide an exhaustive list of material modifications. In general, though, DHS expects that material modifications would likely include changes at a facility to chemical holdings (including the presence of a new chemical, increased amount of an existing chemical, or the modified use of a given chemical) or to site physical configuration, which may (1) substantially increase the level of consequence should a terrorist attack or incident occur; (2) substantially increase a facility's vulnerabilities from those identified in the facility's Security Vulnerability Assessment; (3) substantially effect the information already provided in the facility's Top-Screen submission; or (4) substantially effect the measures contained in the facility's Site Security Plan.

2. Submitting a Site Security Plan

Comment: Several industry commenters recommended changes to the proposed process for notifying facilities to submit SSPs and the timing for submitting the SSPs. A number of commenters believed that the most appropriate person to submit an SSP is a corporate representative with first-hand knowledge of security matters at the facility, rather than an officer of the corporation, as proposed. The comments recommended

allowing a corporate security contact, a security manager, or a consultant with delegated authority to submit information on behalf of the corporation. The commenters indicated that, in most instances, members of senior management teams do not have day-to-day detailed knowledge on security issues and, thus, cannot meet the proposed qualifications. One of the commenters added that the proposed regulations appear to limit an organization's flexibility to assign internal responsibilities for various aspects of the regulations. Another commenter suggested that, in addition to notifying a covered facility, the Department should notify the facility's corporate ownership (and/or parent corporation) allowing a multi-facility corporation to prepare and submit a response in an efficient and timely manner.

Response: The goal of this rule is to increase flexibility while embracing security for covered facilities, not to unnecessarily decrease flexibility. The rule obligates the chemical facility to submit the Site Security Plan; however, as used herein, the term chemical facility or facility shall also refer to the owner or operator of the chemical facility. While the owner or operator of a chemical facility may designate someone to submit the Site Security Plan, the owner or operator is responsible for satisfying all the requirements under this part. Note that the Department has added requirements for submitters in the rule (see §27.200(b)(3)) and that the Department discusses those new requirements in the Rule Provisions discussion of § 27.200. See § II(B). Finally, it is presumed that the covered facility is the most appropriate party to notify its parent corporation or other related corporate entities as necessary.

3. Content of Site Security Plans

Comment: One commenter stated that, until some of the initial regulatory

elements regarding definition of risk and the establishment of tiers is in place, it would be premature for DHS to publish details on Site Security Plans. Another commenter stated that, based on the consequence assessment, every site should be required to have specific security elements in place that prudently deter, detect, delay, and respond based on their assigned tier level. The commenter also stated that, without some degree of access control and physical security specificity based on tier levels, there will be considerable confusion as to the exact considerations needed to meet Department requirements. Another commenter encouraged DHS to abide by the congressional mandate of Public Law 104-113, as described in OMB Circular A119, and ensure that voluntary consensus codes and standards are used when they are applicable under the rule.

Response: The Department has developed a means of assessing risk and a tiering process as described in §§ 27.205 and 27.220. These methods anticipate, on a risk basis, a certain level of vulnerability for a given tier level. A facility's SSP will describe the appropriate levels of security measures that a facility must implement to address the vulnerabilities identified in their SVA and the risk-based performance standards for their tier. The Department has included risk-based performance standards in this interim final rule and will publish further guidance on the risk-based performance standards. The risk-based standards address, among other things, vulnerabilities under the security concepts of detection, deterrence, delay, and response. Finally, the Department notes that covered facilities may use and cite voluntary consensus codes and standards in their SVAs and SSPs to the extent they are appropriate.

4. Approval of Site Security Plans

Comment: In general, commenters supported the proposed submission and

approval processes for SSPs. While one commenter endorsed proposed § 27.240(a)(3) stating that the Department will not disapprove an SSP based on the presence or absence of a particular security measure, another commenter believed that the Department should have the authority to disapprove an SSP if a facility has refused to include a widely-practiced and cost-efficient procedure that can severely reduce the risk posed by a chemical facility. Two commenters requested that the Department inform local law enforcement and first responders when the Department is reviewing an SSP in their community and then inform them whether that plan was accepted or rejected. The commenters stated that the health and safety of responders may well depend upon whether the chemical facility has an adequate SSP.

Response: The Department may not disapprove a Site Security Plan submitted under this Part based on the presence or absence of a particular security measure, as provided in Section 550 of the Homeland Security Appropriations Act of 2007. The Department may disapprove a Site Security Plan that fails to satisfy the risk-based performance standards established in § 27.230.

The Department intends to work closely with local law enforcement and first responders to provide adequate homeland security information to them under this rule.

Comment: One commenter recommended that the Department first complete the SSP review and approval process for Tier 1 facilities, then, after soliciting feedback from the Tier 1 facilities on the process, then proceed in a step-wise fashion to subsequent tiers.

Response: The Department will implement the rule in a phased approach but will not necessarily complete all Tier 1 sites prior to undertaking plan review and approvals

with lower-tier chemical facilities as the need arises. This is necessary to make sufficient progress with higher-tier chemical facilities and not only the highest tier.

5. Timing

Comment: One concern raised by an industry association related to DHS's resources for reviewing Security Vulnerability Assessments and providing responses in 20 days. Changes to control systems were suggested for reviews and updates within 7 days or sooner. One commenter agreed with updating SSPs annually, but not Security Vulnerability Assessments. Several commenters suggested the following for updates: every 2-5 years for Tier 1 facilities, 3-5 years for Tier 2, and 3-7 years for Tier 3 and beyond.

Numerous reviewers recommended that the reviews be limited to approximately every three years. Two companies and one industry association wanted reviews to follow major changes and not follow a set schedule. Many reviewers wanted periodic replaced with a suggested frequency.

Several commenters stated that the requirement to submit SVAs within 60 calendar days, and SSPs within 120 calendar days, starting on the date that the facility is notified that it is considered high-risk, is too short, and therefore inadequate. One commenter noted that managing change in a safe fashion requires significant thought and careful planning to ensure that the change itself does not create another hazard to the community, the environment, or employees. The commenter also noted that developing and implementing an SSP that properly mitigates risk requires the security manager to make appropriate revisions to existing facility procedures and to train employees and other affected parties on these new procedures. Another commenter expressed concern

that there is no specific date or time by which DHS must notify high-risk chemical facilities of their status. Likewise, there is no firm time by which the Secretary will send out a notice approving or disapproving an SSP.

With regard to the time needed to review an SSP, one commenter stated that DHS should issue a decision approving or disapproving them within 30 days of receipt of a completed plan. This timeframe would bring at least most priority facilities into compliance within seven months of the effective date. The commenter also stated that, given the urgency, any "objections" or "appeals" should be processed after the seven-month schedule is completed. Because of concern that DHS staffing levels might delay the processing of SSPs, another commenter requested a provision be included in the interim final rule indicating that facilities are deemed in compliance after 30 days of submission of SVAs and SSPs until such time that the Department reviews and responds to the submission.

A few commenters recommended that the deadline for Tier 1 facilities to submit SSPs be extended from 120 days to 180 days. The commenters believe that this extension would assure facilities adequate time to assemble the best teams, prepare thorough SVAs, deal with budget planning for potentially large capital expenditures, and ensure the on-site work is properly conducted. Another commenter agreed that the proposed submission schedule for submitting SSPs was unrealistic in light of the tasks involved. The commenter also thought that, if DHS found fault with a provision of the SVA, it would be unreasonable to begin development of an SSP based upon a potentially flawed assessment. Consequently, the commenter argued that the submission time of 120 days should be started only after the Department's approval of the SVA is formally

received. Yet another commenter believed that submission of SSPs should be timed according to the tier assigned to the facility and that the time clock should begin when the facility receives word back from the Department on its preliminary tier assignment.

Response: The Department has established a schedule for activities under this part that considers the need to generally address the risks associated with higher tier facilities before that of lower tiers, but staggers the submittals and review and inspection activities. The Department has developed the Chemical Security Assessment Tool (CSAT) to assist chemical facilities with all of the program requirements (registration, screening, SVA, and SSP). In addition, because information from the CSAT applications will be in electronic form, DHS will be able to expedite its review of the information that chemical facilities submit. These deadlines are both prudent and achievable. DHS expects that it will complete its review of the Top-Screen, SVA, and SSP within 60 days of the facility's submission of the Top-Screen, SVA, or SSP.

6. Alternate Security Programs

Comment: The use of alternate security programs was supported by several chemical companies and associations as well as companies and associations in related industries. A chemical company agreed with the concept of initially allowing multiple methodologies and then switching to a common methodology for at least the Tier 1 facilities; they encouraged DHS to still allow alternate approaches for other tiers. This viewpoint was echoed by at least one association. Several companies wanted to ensure that existing plans could be used and one association noted that more methodologies than just those approved by the Center for Chemical Process Safety (CCPS) would be

appropriate. Commenters also noted that CCPS should not be the sole arbiter unless DHS periodically reviews its resources and expertise.

A number of industry associations offered their own approaches and a food industry association commented on the need to keep their current programs in place and to not unduly focus on ammonia refrigeration risks. MTSA-, Sandia-, and NFPA-approved programs were among those mentioned by the commenters, as were those allowed under other regulations. Some commenters found the specific process for approval of alternative programs to be lacking in detail. One association requested that submitters just send in a form saying they have an alternate security plan, and not require any other document be submitted for approval.

An advocacy group commented that alternate approaches needed to be equivalent to the DHS approach, not just sufficiently similar, and that DHS should approve equivalent State and local programs. Another advocacy group suggested that DHS should only determine equivalency based on reviews of individual SSPs, not in any blanket or broad way. A third advocacy group supported a single, consistent approach set out by DHS with private sector programs being modified to conform to the DHS approach. One commenter noted that the specification of RAMCAP may have created an unfair playing field for other firms wanting to visit the source company for RAMCAP.

Response: The Assistant Secretary will review and may approve an ASP upon a determination that it meets the requirements of this regulation and provides an equivalent level of security to the level of security established by this part. In its ASP submission, a facility will have to provide sufficient information about the proposed ASP to ensure that the Department can adequately perform a review and make an equivalency determination.

As described below, certain facilities may submit an ASP in lieu of an SVA, an ASP in lieu of a SSP, or both. Accordingly, the ASP option will only be available following the facility's submission, and Department's review, of the Top-Screen. An ASP for an SVA will need to satisfy the requirements provided in § 27.215, and an ASP for an SSP will need to satisfy the requirements provided in § 27.225. The ASP for the SSP will need to describe specific security measures, or metrics for measures, that will allow the ASP to be considered equivalent to an individually-developed SSP, and facilities implementing an ASP will be subject to DHS inspection against the terms of the ASP.

At this time, the Department will only permit Tier 4 facilities (found to be Tier 4 facilities following the Department's preliminary tiering decision pursuant to § 27.220(a)) to submit an ASP in lieu of an SVA. Tier 4 facilities may submit for review and approval the Sandia RAM for chemical facilities, the CCPS Methodology for fixed chemical facilities, or any methodology certified by CCPS as equivalent to CCPS and has equivalent steps, assumptions, and outputs and sufficiently addresses the risk-based performance standards and CSAT SVA potential terrorist attack scenarios. The Department is requiring Tier 1, Tier 2, and Tier 3 chemical facilities to use the CSAT SVA methodology for preliminary and final tiering. As discussed above in the summary of changes to Rule Provisions, this will provide a common platform for the analysis of vulnerabilities and will ensure that the Department has a consistent measure of risk across the industry. With respect to SSPs, the Department will permit facilities of all tiers to submit ASPs to satisfy the requirements of this rule.

The Department modified § 27.235 to reflect these requirements. The Department also amended the regulation to link the review and approval procedures for ASPs to the review and approval procedures for SVAs and SSPs.

D. Risk-Based Performance Standards

In the Advance Notice, DHS sought comment on the use of risk-based performance standards to address facility-identified vulnerabilities. The Advance Notice proposed that DHS require covered facilities to select, develop, and implement security measures to satisfy the risk-based performance standards in § 27.230. The measures sufficient to meet these standards would vary depending on the covered facility's risk-based tier. Facilities would address the performance standards in the facility's Site Security Plan, and DHS would verify and validate the facility's implementation of the Site Security Plan during an on-site inspection.

1. General Approach to Performance Standards

Comment: The majority of the commenters supported the proposed regulatory approach due to the flexibility that the risk-based performance standards provide to the regulated community in choosing security measures for their respective facilities. The proposed approach acknowledges the fact that each of the facilities faces different security challenges. A few commenters noted that the goal of the performance standards should be to reduce vulnerabilities identified in the SVA, not necessarily reduce all potential consequences or mandate the use of specific countermeasures.

By contrast, some other commenters opposed the Department's proposed regulatory approach, noting various reasons: that the Advance Notice was too prescriptive in certain areas; that performance standards are open to interpretation and

thus can become discretionary, interpretive, and sometimes arbitrary; that chemical companies may be allowed under the rule to make risk reduction determinations based on their available risk reduction budget, rather than on the actual elimination or reduction of the most serious risks; that the rule allows enormous flexibility and variability in the documents that facilities can submit to the Department, which could make program review difficult and hinder any comparative analysis of risk reduction efforts among similar sites.

Response: The Department's statutory authority mandates the issuance of performance standards. Section 550 requires the Department to issue interim final regulations "establishing risk-based performance standards for security chemical facilities." See § 550(a). Also, as noted in the Advance Notice, Executive Order 12866 also directs federal agencies to use performance standards. See 71 FR 78276, 78283. Performance standards avoid prescriptive requirements, and although they provide flexibility, they still establish and maintain a non-arbitrary threshold standard that facilities will have to reach in order to gain DHS approval under the regulation. The ultimate purpose of the performance standards is to reduce vulnerabilities, and that is regardless of risk reduction budgets.

With respect to documentation, except as provided in § 27.235 for Alternative Security Programs, DHS is requiring facilities to electronically submit all documentation required for analysis and approval. Facilities will complete the Top-Screen, Security Vulnerability Assessment, and Site Security Plans through the online, web-based CSAT system. This electronic submission will minimize the variability concerns and allowing DHS to manage and protect information.

Comment: Regarding the application of the performance standards, some commenters thought that facilities should not have to address all performance standards (listed in § 27.230) in their Site Security Plan and should only have to address those performance standards that directly apply to its facility and its risk-based tier. One commenter thought that, in certain circumstances, a covered facility should be able provide adequate chemical security without implementing every one of the risk-based performance standards. The commenter stated that the regulations should allow for situations where the facility can demonstrate that, under its particular circumstances, one or more of the risk-based performance standards is unnecessary or redundant.

Response: Congress intended for the performance standards to provide facilities with a degree of flexibility in the selection of security measures, and the Department has tried to provide that flexibility throughout the rule. DHS expects that a facility will need to address only those performance standards that apply directly to their facility. In addition, DHS notes that there may be circumstances in which a facility needs not implement one or more of the risk-based performance standards and will still be able to provide adequate chemical security; the Department will work with these facilities on a case-by-case basis in these specific situations.

Comment: Several commenters stated that the proposed standards do not include clear security goals, outcomes, or results to measure increased security. They also asserted that DHS should develop a measurement of vulnerability or risk reduction. One commenter suggested that chemical facilities should identify operational and protection goals and that the protection system should be evaluated with respect to meeting these goals. Another commenter suggested that DHS express the performance standards in

terms of overall vulnerability scores as measures via a common Security Vulnerability Assessment methodology. This alternative would allow facilities to devote their security expenses to those measures that would produce the greatest vulnerability reductions and would result, nationally, in the greatest amount of overall vulnerability reduction per dollar spent.

Response: DHS intends for the risk-based performance standards to provide facility owners with the flexibility to choose security measures in their Site Security Plan that will reduce the facility's level of risk. The Security Vulnerability Assessment process, and DHS's resulting placement of the facility within the tier structure, will provide facility owner-operators with an indication of their level of risk.

Comment: Many commenters supported DHS's intention to issue guidance to assist the regulated community in the interpretation and application of the proposed performance standards. They encouraged the Department to work with the regulated community on the development of such guidance. However, some of these same commenters also emphasized that, to effectuate Congress' intention that the chemical security requirements be risk-based performance standards rather than prescriptive requirements, DHS must explicitly make the guidance non-binding. Consistent with the comments about CVI, one commenter discussed the importance of limiting public access to the completed guidance since it could serve as a roadmap for terrorists.

Response: DHS intends to release non-binding guidance on the application of the performance standards in § 27.230 to the risk-based tiers of covered facilities. This guidance will contain sensitive information concerning anti-terrorism measures, and DHS will make that guidance available to those individuals and entities with an appropriate

need for the document. DHS will provide the guidance to the House of Representatives Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs.

2. Comments about Specific Performance Standards

Comment: Several commenters requested clarification about the performance standards in proposed § 27.230(a). A few asked whether paragraph (a)(5) is intended to cover all Department of Transportation hazardous materials and whether it is intended to cover transportation and storage of hazardous materials. One suggested that paragraph (a)(5) should include a provision for securing and monitoring the storage of hazardous materials, in addition to securing and monitoring the shipping and receipt of hazardous materials. Commenters also requested that DHS have facilities report significant security incidents to local law enforcement in addition to the Department. Another commenter indicated that the Department should require the following additional elements in the performance standards: written job descriptions for security personnel, adequate response teams and resources, safe shutdown procedures, evacuation procedures, and decontamination facilities. In addition, another commenter asked that DHS define "dangerous substances and devices" as used in § 27.230(a)(3)(i), "potentially dangerous chemicals" as used in § 27.230(a)(6), and "significant security incidents" and "suspicious activities" as used in §§ 27.230(a)(15) and 27.230(a)(16). Another commenter asked to whom facilities should report "significant security incidents."

Response: These comments relate to the measures that facilities must select, develop, and implement in their Site Security Plans. The Department will provide information in guidance to facilities on these measures. That might include information

on the meaning of these terms, details on the parties to whom facilities should report security incidents and suspicious activities, and explanations about the role of local law enforcement (e.g., the Department's recognition that some investigations of potentially illegal conduct may be the role of local law enforcement).

In addition, DHS also notes that it has made a few changes to the regulatory context based on these comments. As discussed in the summary of regulatory text changes, the Department has revised paragraphs (a)(5), (8), (12), and (15).

Comment: Several comments discussed the need for approaches that address cyber security risks, with several asserting that it is not sufficient for DHS to consider security only from a physical perspective. Commenters opined that there were very few specific references to cyber security in the Advance Notice, even though it is important. Some commenters suggested that DHS should address cyber security in more detail in its own performance standard (i.e., a performance standard that only addresses cyber security), while others suggested that DHS should integrate cyber considerations into other performance standards. Other commenters asked DHS to identify the scope of "cyber" security and "other sensitive computerized systems" in paragraph (a)(8).

Commenters also raised other issues related to cyber security. One commenter mentioned that cyber or joint physical/cyber intrusions could create dangerous chemicals that did not previously exist. Consequently, commenters thought that DHS should address these contingencies in the screening process and/or issue an expansive list of chemicals. Other commenters noted that the RAMCAP approach was not designed to address control system cyber security. A few other commenters believed that the tiering approach is not appropriate for cyber security of control systems. Additionally,

commenters mentioned that it is important to consider that facilities with interconnecting electronic systems could face additional threats as one site's vulnerability poses a risk to other connected sites.

Response: The Department recognizes that cyber security is an issue and has included cyber security as one of the performance standards that facilities must address in their Site Security Plans. Paragraph (c)(8) requires facilities to select, develop, and implement measures that "deter cyber sabotage." In addition, the Department notes that it has implemented an assessment of cyber vulnerabilities for industrial control systems within the CSAT Security Vulnerability Assessment. The Department has accomplished this through the assistance of DHS's National Cyber Security Division (NCSD). DHS appreciates the complexity and uniqueness of addressing cyber security with chemical facilities and anticipates that the CSAT will mature over time, especially with the constructive feedback from interested and knowledgeable parties.

Comment: The Department received numerous comments on its use of the acronym "SCADA" in § 27.230(a)(8). Commenters asserted that SCADA refers to a central control system that monitors and controls a complete site or a system spread out over a long distance. They noted that using the term SCADA to represent cyber systems at chemical facilities is too narrow and suggested that the Department should replace the term SCADA with "Industrial Control Systems."

Response: While the Department had used the acronym "SCADA" (Supervisory Control and Data Acquisition) in the Advance Notice as shorthand for instrumented control systems in general, the Department agrees with the comments and has incorporated broader, more descriptive terminology into this performance standard. The

Department has revised § 27.230(a)(8), so that it reads as follows: "Each covered facility must select, develop, and implement measures designed to: . . . [d]eter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS), critical business systems, and other sensitive computerized systems."

3. Variations in Performance Standards for Risk Tiers

Comment: Several commenters supported the use of risk-based tiers, with several recommending that DHS consult with industry in the development of specific performance standards for each tier. Various commenters favored the Department's proposal to place high-risk facilities in risk-based tiers and to prioritize the implementation phase-in and the level of regulatory scrutiny (i.e., frequency of regulatory reviews, inspections and SVA/SSP updates) based on the facility's risk and associated tier. Commenters noted that DHS should require facilities in higher risk tiers to develop more robust measures to meet the performance standards.

In contrast, a few other commenters had differing opinions. A small number of comments cautioned that performance standards should be consistent across all tiers, regardless of the level of risk. These commenters noted that DHS should adjust the specific measures, not the performance standards, to match the level of risk. In addition, one commenter stated that DHS should not establish risk-based tiers and should instead identify the criteria for those facilities that will be regulated and those that will not. If DHS were to establish tiers, that commenter thought DHS should limit the tiers to high or low risk.

Response: As discussed above in Section III(B)(3), DHS is creating four risk-based tiers, with the highest risk facilities in the top tier (i.e., Tier 1). The types and intensity of security measures (sufficient to satisfy the risk-based performance standards in the facility's Site Security Plan) will depend on the facility's tier. For facilities that present the greatest degree of risk, more rigorous security measures will be needed to satisfy the performance standards. The Department will use a higher level of regulatory scrutiny for facilities that present the highest risk.

DHS consulted with the chemical industry in developing the tier system and performance standards. In adopting the four tier system and applicable risk-based performance standards, DHS intends to employ a scalable performance standard across the tiers, i.e., within the same performance standard, a more robust set of security measures will be needed for a Tier 1 facility than for a Tier 2 facility, for a Tier 2 facility than for a Tier 3 facility, and so on. DHS will ensure that risk-based performance standards are applied consistently across each tier, but guidelines for each tier will vary.

Comment: A few commenters also supported the idea that a facility, which the Department has previously determined is "high risk," can request that the Department move it to a lower tier if it has materially altered its operations in a way that significantly lowers its potential vulnerabilities and consequences.

Response: Pursuant to § 27.205(b), "if a covered facility previously determined to present a high level of security risk has materially altered its operations, it may seek a redetermination by filing a Request for Redetermination with the Assistant Secretary, and may request a meeting regarding the request." DHS has retained that provision in this interim final rule. This provision allows DHS to re-evaluate risk based upon changes at

the facility in process, chemistry, or other factors. DHS, through the Assistant Secretary, intends to evaluate such proposed measures on a case-by-case basis.

In evaluating the redetermination, DHS will consider whether the planned action actually reduces risk (as opposed to simply "moving" the risk into the community around the facility) and does so without compromising security. Where these parameters are met, DHS will approve the plan and re-evaluate the tier placement for the facility in question. Pursuant to § 27.205(b), the Assistant Secretary will notify the facility of the Department's decision on the Request for Redetermination within 45 calendar days of receipt of such a Request or within 45 calendar days of a meeting regarding the Request.

Comment: One commenter noted that how performance standards vary across tiers would depend on the criteria used to establish the tiers.

Response: DHS will assess all facilities based upon worst plausible case scenarios as applicable to each facility.

4. Adoption of MTSA Provisions

The Advance Notice solicited comment on whether DHS should adopt various provisions from MTSA as elements of the chemical security program. In particular, DHS asked whether it should adopt the following performance standards in addition to the standards already listed in 6 CFR § 27.230: 33 CFR § 105.250 (Security systems and equipment maintenance), 33 CFR § 105.255 (Security measures for access control); 33 CFR 105.260 (Security measures for restricted areas); 33 CFR § 105.275 (Security measures for monitoring); 33 CFR § 105.280 (Security incident procedures). See 71 FR 78276, 78284.

Comment: Of the several comments received on the request, the majority opposed adopting the standards, characterizing them as highly detailed and prescriptive and, as such, incompatible with the risk-based performance standards proposed for chemical facilities. A chemical industry association presented an analysis of the four MTSA standards and concluded that they were largely duplicative of, or potentially inconsistent with, existing categories of performance standards presented in the Advance Notice. The commenter stated that the MTSA standards were not performance standards, but mandatory particular security measures, in direct conflict with Section 550. Through a similar section-by-section analysis of the MTSA provisions, a chemical manufacturer found several provisions to be compatible with performance standards, but others too prescriptive or incompatible with activities in chemical facilities.

Another association representing chemical distributors stated that only a tiny fraction of its members relied on waterways to distribute chemicals and, accordingly, recommended against adoption of the standards.

Response: The Department agrees with the commenters who recommended against adopting the MTSA provisions referred to in the preamble of the Advance Notice. As the commenters noted, these provisions either duplicate current standards, conflict with current standards, or mandate particular security measures in conflict with the statute.

Comment: One association noted that, because many of its members had facilities on waterways, member companies often developed MTSA-type approaches to Security Vulnerability Assessments and Site Security Plans to establish some uniformity across facilities. Another commenter suggested that when an owner of multiple facilities

has some covered by MTSA and other by the chemical security rules, MTSA could be an ASP if applied to non-MTSA facilities.

Response: Where the application of MTSA practices is sufficient, it may be considered a valid ASP. DHS will review and consider adoption of MTSA plans to non-MTSA facilities on a case-by-case basis. The Department does not intend to require duplication of effort where responsible facilities have implemented adequate security measures.

E. Background Checks

Under the Advance Notice, covered facilities would be required to perform appropriate background checks on and ensure appropriate credentials for facility personnel and, as appropriate, for unescorted visitors with access to restricted areas or critical assets.

Comment: Numerous commenters stated that chemical facilities already screen their employees for their own interests and in response to government programs. The commenters urged that the level of screening for existing employees and contractors should be commensurate with the access provided. While some commenters wanted existing employees who had undergone employee screening before hire to be "grandfathered" from any new requirements, other commenters thought that existing employees should be subject to screening when they are assigned to secure areas or have the potential to be reassigned. An association recommended checking current employees with less than five years seniority within six months of the effective date of the program and more senior employees within one year.

Several commenters argued that, extending the proposed requirements to

contractors, subcontractors, truck drivers, and delivery and repair personnel, and others who are frequently on site, would create serious difficulties because of the large numbers of individuals in these categories, the need to have them available on short notice, redundancy of existing credentials, cost of new credentialing, and delay while screening is completed. Chemical companies explained that they rely heavily on contractors and expect the contracting company to be responsible for assuring that their employees meet security requirements. Commenters suggested that officers hired by the facility supervise contractors and sub-contractors without background checks.

The commenters also addressed the types of background checks that DHS is considering, including the personal information required, and whether name checks against the Terrorist Screening Database and fingerprint-based checks for terrorism, criminal history, or immigration status would be required. A number of commenters urged DHS to tailor the degree of scrutiny to the degree of employee access to sensitive locations. Private screening firms described systems that collect more detailed information and enhanced verification depending on the applicant's access. Operators of private screening systems state that they typically rely on the database screens for candidates with potential terrorist connections. A chemical industry association supported screening of chemical facility employees for terrorism, criminal records, and immigration status.

One commenter explained that biometric testing in a chemical environment can fail because of smudging and deterioration of fingerprints over time, while another believed that adequate field testing had not been completed. Another commenter explained that biometrics and other verification techniques will not foil a person who has

stolen an identity to pass the screen. The commenter recommended that authentication techniques, in addition to validation and verification, be applied to applicants with access to secure locations. In response to the proposed use of a list of disqualifying crimes to reject applications for clearance, a number of commenters urged DHS to restrict the crimes to those that were most clearly linked to potential for terrorism. The commenters, both unions and chemical companies, argued that loyal employees can lose their jobs or fail to qualify for hire because of misdemeanors, such as missing a few months of child support, or crimes that are not good predictors of the potential for terrorism. One commenter recommended adoption of an appeal process that allows a disqualified person to explain why he or she is no longer at risk, similar to the process under MTSA regulations.

The preamble also requested comment on whether the access provisions of the Transportation Worker Identification Credential (TWIC) Program, Hazardous Materials Endorsement (HME), ATF requirements, or other structured programs should apply to chemical facility security programs. A few commenters supported the concept that the screening required for the TWIC program should be acceptable for the chemical security program. Indeed, many chemical facilities are on bodies of water and employees were already compliant with the TWIC program. Another commenter took the opposite position that the TWIC program did not provide the customization available in existing screening systems to grade the level of screening based on employment and assignment decision. Numerous comments maintained that an employee or contractor who was credentialed under the TWIC, HME, ATF, or similar programs should not need additional security screening under the chemical security program. Related comments

requested portability of security checks for employees or contractors cleared by another chemical facility. One commenter recommended that DHS establish a national repository of cleared personnel to minimize redundancy and expense.

With respect to the question of whether the government should conduct background checks or whether the industry could use authorized third parties to conduct the checks, three commenters stated that third parties were already providing background checks for thousands of employees of chemical facilities. Other commenters, including organizations that provided screening services, maintained that existing programs for screening applicants and employees for chemical facilities were reliable, effective, and inexpensive. Another commenter wrote that one program operated through safety councils might be eligible as an alternate security program, although a chemical company suggested not using safety councils, because their standards were too lax.

A few commenters favored the government's undertaking background checks because, unlike private companies, the government has access to terrorist databases and FBI databases, and because the government, unlike employers, would be immune from legal challenges from a rejected employee. Opposition to government responsibility came from several commenters who were concerned about slow completion of background checks, and that the backlog might be exacerbated by a new chemical security program.

A few commenters, including three unions, strongly urged that the system provide an appeals process for affected applicants whose employment prospects in the chemical industry and elsewhere could be seriously affected by an erroneous determination. Private services noted that they notified applicants of adverse decisions and allowed them

to contest the decisions.

Response: DHS believes that personnel surety is a key component of a successful chemical facility security program. This component of the performance standards will enhance security in what would otherwise be a significant potential vulnerability. In the Advance Notice, the Department requested comment on these components of a background check program: (1) What individuals should have a background check? (2) When should the check be required? (3) What type of background check should be conducted? And (4) Should the federal government conduct the check? We address each of these four issues below.

First, DHS agrees that the level of screening for employees and contractors should be commensurate with the access provided. As part of this approach, the facility shall identify critical assets and restricted areas and establish which employees and contactors may need unescorted access to those areas or assets, and thus must undergo a background check. A facility's approach to personnel surety, including its defined restricted areas, its critical assets, and a list of the employees requiring background checks, shall be detailed in the Site Security Plan that the facility submits to the Department for approval. The rule does not include a provision that would exempt certain employees from the personnel surety performance standard based on length of employment at the facility. Merely because an individual has worked in a chemical facility for a period of time without incident does not automatically mean that they do not pose a terrorism risk and should be given free access to restricted areas and critical assets without a background check. Allowing such access without a background check presents an unacceptable security risk, and is contrary to the performance standard on personnel surety. This is not

to say, however, that employers may not consider an employee's prior history of employment and service in making personnel decisions. It should also be noted that nothing in this regulation prohibits a person that has been convicted of a misdemeanor offense from being employed at a high risk chemical facility.

Second, DHS views the background check process as one of the many pieces of the Site Security Plan, and as such, will require that it be completed and submitted with the Site Security Plan. Once the facility receives the Letter of Authorization under § 27.245 denoting preliminary approval of the Site Security Plan, the facility may then proceed with all necessary background checks, if it has not done so already. All employees required in the SSP to have a background check should be included in the initial submission and must be duly vetted in accordance with the plan. This should not cause any interruption in work.

Third, the Department understands that many covered facilities already perform background checks on employees and certain contractor employees, and with some modifications, will allow that process to continue. In order to perform an appropriate background check for the purpose of protecting critical assets and restricted areas of high risk chemical facilities from persons who pose a terrorist threat, the Department has made some modifications to the personnel surety performance standard in the regulation. The Department will consider appropriate open source background checks as an acceptable response to the background check performance standard. Specifically, the Department will consider as appropriate a background check process that verifies and validates identity; includes a criminal history check of publicly or commercially available databases; verifies and validates legal authorization to work through the I-9 process; and

includes measures designed to identify people with terrorist ties. This last standard can be achieved by checking against the consolidated Terrorist Screening Database (TSDB). The Department modified the performance standard at 6 CFR § 27.230(a)(12) to reflect these changes.

Fourth, while much of the background check process can be accomplished by commercial methods, the check of the Terrorist Screening Database is an inherently governmental function that necessarily includes a check of classified databases that are not commercially available. The Department will augment the background check in the SSP with a TSDB check. The Department has determined a TSDB check is necessary for the purpose of protecting critical assets and restricted areas of high risk chemical facilities from persons who pose a terrorist threat.

DHS will designate a secure portal or other method for the submission of application data for each employee or contractor for whom a TSDB check is required in the SSP. The Application data will be the name, date of birth, address, and citizenship, and if applicable, the passport number, DHS redress number,[1] and information concerning whether the person has a DHS credential or has previously applied for a DHS credential.

To minimize redundant background checks of workers, DHS agrees that a person who has successfully undergone a security threat assessment conducted by DHS and is in possession of a valid DHS credential such as a TWIC, HME, NEXUS, or FAST, will not

[1] A DHS redress number is issued by DHS to an individual who has successfully completed a redress inquiry, in which the inquiry resolved a previous false-positive match to a watch list record. Redress inquiries can be submitted directly to DHS as part of the DHS Traveler Redress Inquiry Program (DHS-TRIP).

need to undergo additional vetting by DHS. Even so, the facility shall submit the name and credential information for these persons along with the application data for other employees. Facilities shall not allow unescorted access to a critical asset or restricted area to a person in possession of a DHS credential unless information on that person has been submitted as discussed above.

DHS will screen each applicant and determine whether the applicant poses a security threat. Where appropriate, DHS will notify the facility and applicant via U.S. mail, with information concerning the nature of the finding and how the applicant may contest the finding. Applicants will have the opportunity to seek an adjudication proceeding and appeal under Subpart C.

F. Inspections and Audits

Numerous comments addressed the proposed provisions for auditing and inspecting chemical facilities to determine compliance and allowing certified third-party auditors to supplement DHS personnel at lower tier facilities. While DHS has responded, to the extent that it is able, to the comments below, DHS also notes that it will issue guidance that identifies appropriate processes for inspections and provides specifics about the records that must be made available to DHS upon request. See §§ 27.250(d) and 27.255. That guidance will provide further detail.

1. Inspections

Comment: Section 27.245(a) in the Advance Notice provided that DHS may "enter, inspect, and audit the property, equipment, operations, and records of covered facilities." One commenter asserted that DHS should inspect and audit using an approved or preliminarily approved Site Security Plan and not on other criteria outside

the scope of the Site Security Plan. In addition, commenters indicated that DHS need not inspect equipment and records related to operations outside the vulnerabilities identified in the facility's Security Vulnerability Assessment and protected in the Site Security Plan; the commenter thought that such inspections would go beyond what is required to ensure that high-risk chemical facilities are secure. In addition, one commenter requested that DHS revise the scope of inspection to property, equipment, operation, and records covered in a facility's Site Security Plan.

Response: During inspections, authorized DHS officials may inspect equipment, view and/or copy records, and audit records and/or operations. This section imposes an affirmative obligation on facilities to cooperate with authorized DHS officials, including inspectors, and allow inspections and audits. DHS will inspect a covered facility following DHS's preliminary approval of the facility's Site Security Plan. DHS may also inspect facilities outside of the Site Security Plan approval cycle if there are exigent circumstances or special security concerns. During the course of inspections, an inspector may ask a facility to demonstrate the effectiveness of a given security measure found in the facility's Site Security Plan. This will help the inspector to determine whether the facility has adequately implemented the risk-based performance standards in its Site Security Plan. With respect to requests for records, the Department expects that facilities will produce the records--whether located onsite at the facility, at corporate headquarters, or in any other location--that are relevant to the security of the facility. The Department has added some additional language in the rule about the production of records. See § 27.250(d)(4).

With respect to scope of inspections, DHS is not narrowing its scope to cover only those items covered in the facility's Security Vulnerability Assessment and Site Security Plan; DHS needs the appropriate discretion to inspect those items and areas that are related to the security of the facility. However, DHS has no intention of inspecting areas that are unrelated to security.

Comment: One industry association noted that § 27.245(b)(1) of the Advance Notice suggested that security measures (which DHS requires for final approval of the Site Security Plan) should be in place at the time that DHS inspects a facility. The commenter stated that, if facilities address vulnerabilities through capital improvements, facilities are unlikely to have these security measures in place within the stated time frame. In such cases, the commenter recommended that DHS use a timeline approach, detailing an implementation schedule of prioritized security measures, and include that timeline in a facility's Site Security Plan.

Response: The commenter is correct in noting that DHS expects that facilities will have met the requirements of § 27.225 (i.e., the facility will have developed and submitted a Site Security Plan, which the Department will have preliminarily approved) when the Department visits the facility for an inspection or audit. See § 27.250(b)(l). One of the purposes of the inspection is for the Department to determine whether facilities have adequately implemented their Site Security Plans.

However, the Department realizes that there may be circumstances where facilities will have to implement security measures through capital improvements, and that can take time. Based on the Department's assessment of risk at a given facility and the realities of getting security measures into place, the Department will work with

facilities on a case-by-case basis. Where the Department believes that extra time is warranted, the Department will work with facilities to incorporate that time into the facility's Site Security Plan and into the Department's timeline for inspecting the facility.

Comment: Various commenters requested clarification about the time and manner provisions found in § 27.245(c) of the Advance Notice. Several commenters noted that the proposed regulations did not define the terms "reasonable times" or "reasonable manner" and asked the Department to define those terms. In addition, some commenters noted that the preamble provided a timeframe for inspections ("during regular business hours of 9 a.m. to 5 p.m.") but that the Advance Notice text did not specify that timeframe. Other commenters indicated that DHS should clearly outline the regularity of audits and inspections that the Department will require for each tier.

Several other comments discussed the notice provisions in the rule. The Advance Notice provided that "DHS will provide covered facility owners and operators with 24-hour advance notice before inspections, except where the Under Secretary or Assistant Secretary determines that an inspection without such notice is warranted by exigent circumstances and approves such inspection." See § 27.250(c). Several industry associations believe that 24-hour advance notice would not be a sufficient amount of time for facilities arrange for the appropriate personnel to be available for the inspection. Commenters suggested that DHS provide more notice to facilities; requests ranged from three to seven days. Other commenters requested that, in addition to notifying the facility, DHS also provide local emergency responders and local agencies tasked with regulating hazardous materials facilities with a 24-hour advance notice as a courtesy.

Others commented on the concept of unannounced inspections. A member of

Congress objected to the restrictions on unannounced inspections, asserting that the provision was a near-preclusion of random audits, because approval by senior officials (i.e., the Under Secretary for Preparedness or Assistant Secretary for Infrastructure Protection) would make unannounced audits exceedingly rare. Moreover, focusing such unannounced audits exclusively on facilities (or geographic regions) where agency officials determine that "exigent circumstances preclude notice" presupposes that the agency is already in a position to know where exigent circumstances exist. As a result it would be far harder for the Department to determine actual rates of compliance with regulatory requirements. An industry commenter would support unannounced inspections for facilities that had significant deficiencies in the prior inspection or that have had an unusual number of breaches.

Response: DHS has retained the language that it used in the Advance Notice. Authorized DHS officials will conduct audits and inspections during reasonable times and in a reasonable manner. The nature of any given inspection will depend on the specific circumstances surrounding a particular facility's operations at a given point in time and will be considered in conjunction with available threat information.

Commenters asked for clarification on the times that DHS plans to conduct inspections. While DHS expects that it will conduct many of its inspections during the regular business hours of 9 a.m. to 5 p.m., DHS will not limit its inspections to regular business hours only. DHS must have the flexibility to respond to information, operations, and circumstances whenever they exist or develop, and so DHS may have to conduct inspections in the evening, at night, or during weekends. Security concerns are different at different times of the day and on different days of the week, and so DHS must able to

able to assess the different security measures that facilities put into place, pursuant to their Site Security Plans.

DHS has maintained the Advance Notice provision that gives facilities 24-hour advance notice before an inspection. In some circumstances, DHS may provide facilities with additional time. As a general matter, DHS believes that 24 hours is an appropriate and reasonable notice period, striking a balance between providing the Department with flexibility to determine compliance with this regulation and providing regulated entities with sufficient notice to prepare for an inspection. Some commenters suggested that DHS also provide advance notice about inspections to local emergency responders and local agencies. While DHS may choose to notify local emergency responders or other agencies on a case-by-case basis, DHS does not believe it is necessary to include a mandatory requirement in the rule.

Many commenters expressed concern that DHS is not able to conduct unannounced inspections. These concerns are unfounded: DHS will be able to conduct unannounced inspections when it complies with internal policy. While DHS has a general requirement for advance notice, DHS recognizes that there may be circumstances where advance notice is not possible.

To accommodate those circumstances, DHS has identified two exceptions. See § 27.250(c). DHS had identified one exception in the Advance Notice: If the Under Secretary determines that an inspection without notice is warranted by exigent circumstances, the Under Secretary or Assistant Secretary may approve such an inspection. The exigent circumstances may include threat information warranting immediate action. DHS adds a second exception in this interim final rule: If any delay in

conducting an inspection might be seriously detrimental to security, and the Director of the Chemical Security Division, Office of Infrastructure Protection determines that an inspection without notice is warranted, the Field Operations supervisor may, permit an inspector to conduct such inspection. This additional exception addresses the concerns of commenters who claimed the exception in the Advance Notice was too restrictive.

Comment: Some commenters noted that facilities may choose to validate any government-issued credential for the purpose of inspectors gaining entry onto a chemical facility. One commenter requested that, as part of the guidance, DHS include information on the security measures that will allow a facility to determine that the DHS officials or third party auditors are legitimate.

Response: DHS will handle this issue like other Federal agencies handle their respective inspectors and auditors. Individuals performing these inspections will carry Federal government credentials identifying themselves as having official authority to inspect. In addition, any chemical facility wishing to authenticate the identity of an individual purporting to represent DHS may contact the appropriate DHS Chemical Security Division official within the Office of Infrastructure Protection at DHS headquarters. In addition, the Department has provided some additional regulation text on the issue of inspector credentials. See § 27.250(d)(1).

Comment: Several commenters addressed the issue of training for inspectors. One commenter stated that it is DHS's role to ensure that inspectors and auditors are qualified in both physical security and chemical processes. Others noted that, if inspectors and auditors do not have a background in chemical manufacturing, then DHS must adequately train inspectors. Furthermore, that commenter encouraged DHS to

utilize a cross functional team consisting of individuals with chemical process knowledge and physical security background and include a local area first responder on each inspection team for each facility. The commenter noted that many facilities maintain a close relationship with local emergency responders. One commenter indicated that DHS inspectors should expect that chemical facilities may require them to complete a safety overview before being granted access to a facility; this is regardless of the training that DHS provides to its inspectors.

Response: DHS will use properly trained personnel to conduct inspections. During inspections, DHS intends to use teams consisting of Federal inspectors, many with backgrounds in law enforcement and physical security, and experts in chemical manufacturing. DHS will put inspectors through a rigorous training program, incorporating both classroom training and on-site visits, so that inspectors are informed on all aspects related to this regulatory program as well as on safety issues. These individuals will receive training on specific safety procedures, including OSHA's Hazardous Waste Operations and Emergency Response Standard (HAZWOPER), that they should use while visiting chemical facilities. If chemical facilities request that inspectors receive facility-specific safety briefings or training, the Department will work with facilities to accommodate those concerns, provided that the additional safety training is reasonable given the nature of the expected inspection.

2. Third-Party Auditors and Inspectors

Comment: Numerous chemical companies, industry associations, and State and local agencies requested clarification on the roles and responsibilities of third-party auditors. Several commenters pointed out that there is currently a lack of standards for

third-party auditors, and some commenters noted that if DHS does not provide specific criteria for compliance, such audits will be very subjective. Several commenters asserted that there is a need for DHS to develop standards and requirements for third-party auditors, including requirements for certification, qualifications, independence, objectivity, training and re-training, confidentiality, ethical obligations, conflicts of interests, discipline procedures, and liability insurance.

Several commenters discussed the third-party auditor certification or approval process in detail. One commenter pointed out that DHS would have to develop either a professional registration or licensing for third-party auditors in order to establish a minimum level of competency for third-party auditors. Other commenters stated that training should include, among other things, information on physical security, chemical processes, and safety operations. One commenter recommended Sandia National Laboratory's Risk Assessment Methodology for Chemical Facilities (RAM-CF) training as an excellent review in all aspects of chemical facility operation and security. One pointed out that there is currently no certification for control system cyber security auditors. Another commenter added that any DHS third-party inspectors should have a strong background and experience with the agricultural retail/distribution segment of the chemical industry. The commenter encouraged DHS to work with industry associations and industry experts on establishing the proper criteria to select certified third-party auditors that will be used to inspect agricultural retail or distribution facilities determined to be covered by these regulations.

One commenter was concerned that DHS had not effectively addressed auditor independence and objectivity in the Advance Notice. To remedy this concern, the

commenter suggested that DHS define third-party auditor and address auditor concepts such as due diligence, due professional care, auditor certification, auditor training, auditor indemnification, conformity assessment, audit/inspection methodology, etc.

Other commenters raised questions about third-party auditors and information protection. One commenter stated that all third-party auditors must be held to the same requirements and standards as applied to DHS officers and employees regarding the protection of confidential information; this includes information protected by law, such as PCII, Sensitive Security Information (SSI), or other applicable requirements. DHS should develop requirements and procedures, including the use of non-disclosure agreements, to prohibit disclosure or use of confidential information developed or obtained during the auditing process. One association, whose member companies already use third party audits, wanted confirmation that the use of third-party auditors would be in compliance with the CVI framework.

Three State agency commenters urged the Department to clarify that the third-party auditor provision includes qualified state and local assets to conduct audit inspections and assist with Security Vulnerability Assessments and Site Security Plans. One commenter would limit third-party auditors to appropriate state and local government officials with familiarity of the chemical process safety and security systems currently in place at the chemical facility in question to ensure the credibility and effectiveness of the inspection and auditing program. Some other commenters suggested that State and local entities could be a resource base for audits and site visits, including those of higher tier facilities.

Commenters asked several other specific questions about DHS's use of third-

party auditors. A chemical company requested clarification on how DHS could delegate its authorities to third-parties. Another commenter wanted the ability to seek legal remedies against third-party auditors. Other commenters raised the question of who would pay for third-party auditors, suggesting that DHS should.

Some commenters argued for the use of third-party audits at any chemical facility regardless of its tier ranking. One commenter noted that the eventual requirements for certification should be stringent, creating confidence that the auditor will be just as capable as DHS inspectors of auditing or inspecting a high-risk facility. The commenter suggested that, as a result, a certified third-party auditor should also be allowed to conduct inspections at "high" or "higher" risk facilities. Other commenters noted that allowing third-party auditors to perform work at any chemical facility, regardless of its tier, will increase the ability of DHS to rapidly and effectively review security plans at chemical facilities by making sure sufficient numbers of inspectors are available at any given time.

Other commenters opposed DHS's use of third-party auditors altogether. A chemical industry commenter opposed DHS's use of consultants, contractors, or vendors to perform audits and inspections of facilities based on concerns about confidentiality and conflicts of interest. The commenter asserted that DHS-trained personnel are best suited to understand the complexities of security in affected facilities and to understand the importance of sensitive business information provided to DHS. Consequently, the commenter urged DHS not to initiate the proposed program without the appropriate level of staff, training, and resources necessary to implement enforcement. One commenter preferred that DHS officials, not officials from other government agencies or non-

governmental organizations, conduct third-party inspections or audits to assess compliance; the commenter asserted that consistency of audits can only be maintained if one agency, using the same inspection and/or audit procedures, performs the work. Several other commenters disagreed with the concept of third-party auditors unless they were under contract to DHS and met DHS hiring standards and training certifications. They felt that if such an activity is important, then DHS should carry out the activity itself.

Response: The Department recognizes that there are many important and complex issues surrounding the use of third-party auditors. Those issues include questions about whether it is appropriate for DHS to use third-party auditors and if so, for which tiers of facilities; what the standards and requirements would be for those third-party auditors; and who would pay for third-party auditors. DHS continues to take these issues under advisement. DHS intends to issue a future rulemaking providing the details about its plans to use third-party auditors. In developing its proposed rule, DHS will consider these comments about third-party auditors. Until that time, DHS will use its own inspectors for conducting inspections and audits.

G. Recordkeeping

Comment: One commenter suggested that the recordkeeping and reporting requirements be strengthened for process malfunctions or any attempted terrorist attack; the need for emergency response, safe shut down, evacuation and decontamination procedures in case of an attack or malfunction be defined; and effective training requirements for workers in covered facilities be required.

Response: Recordkeeping requirements under this new authority focus on security and will capture many of the issues identified by the commenter. Recordkeeping requirements regarding incidents under process safety, including shut down/start up, are outside of the scope of this regulation.

Comment: One commenter asked for guidance regarding what would constitute a reportable "security incident" or "suspicious incident." The commenter noted that DOT has provided helpful guidance for reporting and recordkeeping under HM-232.

Response: The Department will provide facility owners with guidance on these and other terms used in the recordkeeping section.

Comment: Another commenter suggested that § 27.250(a)(4) include a reference to NFPA 731, Standard for the Installation of Electronic Premises Security Systems (2006 edition), Chapter 9, Testing and Inspections. The commenter supported the recommendation by pointing out that all NFPA codes and standards are developed through the voluntary consensus process and are accredited by the American National Standards Institute (ANSI); that Congress, in several cases has mandated the adoption of NFPA codes and standards and that Public Law 104-113, as described in OMB Circular A119, mandated that voluntary consensus codes and standards be used when they are applicable and to ensure that chemical facility safety be the primary concern.

Response: Voluntary consensus approaches to chemical facility security will be addressed in guidance. However, the Department cannot mandate specific security measures under this authority.

Comment: One chemical association found the requirements for recordkeeping to be excessive. Concerning training, the commenter stated that the location of the session

and the name and qualifications of the trainer were not important, and the requirement for attendees' signatures would cause headaches if attendees leave without signing. Also, many of these requirements seem to prevent the use of web-based training. With respect to the drill and exercise provision, the commenter believed that a comprehensive list of participants is more challenging than it might appear, since drills and exercises frequently involve persons in multiple locations. Finally, recording the name and qualifications of every maintenance technician is overly burdensome and extremely difficult to document. According to the commenter, this proposed requirement would lead to inadvertent non-compliance due to its inherent complexity. The commenter urged that the recordkeeping requirements, at most, track the MTSA requirements (33 CFR § 105.225), which are less detailed and only require records to be maintained for two years.

Response: Memorializing minimal information about training, drills, exercise, and maintenance is important for a facility to assist in the analysis and review of its security efforts, and DHS does not agree that these requirements are overly burdensome or excessive given the potential risks in this sector. The recordkeeping requirements address specific issues that arise in chemical facilities, and a three year period is consistent with the anticipated audit and review cycle under this rule.

Comment: An industry association argued that, in light of existing DOT requirements, no additional training and recordkeeping requirements are needed for battery transportation. Further, any training and recordkeeping requirements that are made applicable to drivers hauling covered chemicals should be the responsibility of the transportation firms, not the facilities they service.

Response: There are no specific requirements for recordkeeping of transportation

activities in this rule.

H. Orders

Comment: Various commenters mentioned the remedies in proposed §§ 27.300, 27.305, 27.310, and 27.315. An industry group indicated that the rule should provide adequate protection for recipients of penalty and cessation orders, including the opportunity for an adjudicatory hearing before a neutral hearing officer. The commenter suggested that the rule make clear that the burden of proof lies with DHS, not the facility; that facilities may be represented by counsel; that the facility is entitled to present evidence on its behalf; that there be an orderly process for the hearing officer to make a decision on the basis of the record presented, including a record of decision and for intra-agency appeal of the hearing officer's decision before it becomes final. Finally, a trade association pointed out a typographical error in proposed §§ 27.305(b) and 27.310(a).

Response: The Department has substantially revised the regulatory text in Subpart C, which includes Orders, adjudications, and appeals. The Department directs commenters to the revised regulatory text in Subpart C, as well as summary of those changes in § II (B) Rule Provisions. In sum, the Department has included adjudicatory procedures for a proceeding before a neutral hearing officer whereby facilities and others may be represented by counsel and may present evidence. The procedures provide that the burden of proof rests with the Assistant Secretary and that a record will be compiled for an appeal within DHS.

Comment: Several others provided input on cessation orders. A local government agency indicated that an Order to Cease Operations likely would be litigated immediately after issuance, and questioned how non-compliance during the lengthy

litigation period would be remedied. Another commenter recommended that DHS add a provision stating that it would not enforce an order to cease operations within 30 days of a final action, which would allow the facility time to seek judicial review. An industry commenter stated that DHS's professional assessment that a chemical facility was in total violation of the security requirements should result in an initial audit of what is required at that particular site to be in compliance. If, after a reasonable time, the facility does not come into compliance, then DHS should consider temporary closure until compliance is attained. An association expressed concern that DHS should consider whether a facility's products are critical to the economy, chemical industry, or national security before imposing fines or issuing a notice to cease operations.

Response: As noted above, the Department has substantially revised the regulatory text in Subpart C, which includes the provisions on Orders, adjudications, and appeals. Consistent with the statement in the Advance Notice, the Department realizes that an Order to Cease Operations would likely be litigated immediately after issuance. See 71 FR 78276, 78287.

I. Adjudications and Appeals

Comment: While commenters generally supported the processes proposed for objections and appeals, some thought that DHS should strengthen and expand the objections and appeals provisions. Several commenters suggested that DHS include additional provisions to the objections and appeals sections. One commenter recommended that DHS revise the rule to include a full description of the administrative review process, including the procedures to which all parties and the adjudicating official

must adhere. Another commenter recommended that the Under Secretary and the Deputy Secretary have the authority to delegate their responsibilities as adjudicating officials.

One commenter stated that the burden of proof should lie with DHS, not the order recipient, that recipients may be represented by counsel, that the recipient is entitled to present evidence on its behalf, that there be an orderly process for the hearing officer to make a decision on the basis of the record presented, including a record of decision, and for intra-agency appeal of the hearing officer's decision before it becomes final.

Response: DHS has reorganized the adjudications and appeals procedures, as discussed in the summary of rule provision changes to Subpart C. See § II(B). Given that the rule already provides consultation opportunities, coupled with the fact that the Department has greatly modified its adjudications provisions, the Department believes it is unnecessary to retain the objections provisions from the Advance Notice (proposed §§ 27.205(c), 27.220(b), and 27.240(c) and has thus removed them from the interim final rule. Of course, consultations are still available pursuant to various provisions in the rule including § 27.120(b).

In addition, DHS now expressly spells out new procedures for adjudications and appeals. In particular, DHS has added adjudicatory procedures for a proceeding before a neutral hearing officer whereby facilities and others may be represented by counsel and may present evidence. The procedures provide that the burden of proof rests with the Assistant Secretary and that a record will be compiled for an appeal within DHS. The Secretary is expressly authorized to appoint individuals to serve as a neutral hearing officer. The Secretary and others retain their existing authority to delegate duties and responsibilities.

Comment: Another commenter suggested that DHS revise the rule to provide some guidance and limitation on the number of requests that a facility will be permitted to make for additional information and on the maximum extent to which DHS will toll timeframes. One commenter noted that although there is authority for the Assistant Secretary to ask the facility for more information, there is no mechanism for the facility to seek further explanation that is needed for purposes of arguing its objection.

Response: The revisions of the procedures substantially address these comments. The adjudications provisions empower a hearing officer to make decisions on the information to be accepted into each hearing record.

Comment: Another commenter stated that, under the Advance Notice, a facility had the option of using the appeal procedure (instead of the objection procedure) for challenging the disapproval of its SSP. The Advance Notice stated that orders are stayed until the administrative appeal is completed, but the Advance Notice did not provide specifically for the disapproval of a SSP to be stayed pending the administrative appeal. The commenter suggested that DHS should make such a stay explicit.

Another commenter argued that, because timelines are short, facilities will be forced to complete the SVA and SSP regardless of the outcome of the appeal, thus rendering the appeals process moot. If a facility objects to a determination, whether it is opposing either the overall assessment of "high risk" or the specific tier assignment, one commenter recommended that DHS should issue a decision on objection before the facility is required to implement any additional measures - including both the SVA and SSP.

Response: The addition of the factual adjudication procedure, with provisions on

the effectiveness of administrative actions during adjudications and appeals, substantially address these comments. The adjudications and appeals sections provide that, absent exigent circumstances, Orders are stayed pending the completion of proceedings.

Comment: Another commenter indicated that §§ 27.205(c)(1), 27.220(b)(1), and 27.240(c)(1 (of the Advance Notice) cite "within 20 calendar days" as the deadline for filing objections regarding the high risk determination, risk-based tiering, and disapproval of site security plans. In contrast, §§ 27.215(c), 27.305(d), and 27.320(b)-(d) (of the Advance Notice) cite "within 30 calendar days" for certain deadlines regarding notification, appeals, and payments of civil penalties. The commenter believed that having two different deadlines for various actions under the regulatory program is burdensome to both DHS and the regulated facilities, and requested that all "within 20 calendar days" be amended to "within 30 calendar days" to provide more consistency within the Department's regulatory program. Another commenter urged that an appeal must be filed within 30 calendar days of when the order is issued should be changed to within 30 calendar days of when the order is served. See § 27.320(b) of the Advance Notice.

Response: The Department's revisions to the adjudications and appeals provisions substantially address these comments. The rule continues to permit consultations but does not set hard and fast time periods for such consultations. See, e.g., § 27.120(b), § 27.240(b), and § 27.245(b). With respect to the time periods for adjudications and appeals, the revised procedures provide that adjudications and appeals must be commenced with stated time periods after "notification." See, e.g., § 27.310(b)(2) or § 27.345(b)(2).

Comment: One commenter recommended that the regulations provide specifically that DHS would make available to the public non-confidential summaries of determinations on appeals. The commenter also recommended that the regulations contain specific statements that objections and appeals may be submitted as CVI.

Response: The adjudication and appeal sections contemplate that the hearing officer or appeal officer will make the necessary decisions concerning the handling of CVI. There is nothing in the procedure to prevent a facility or other person from relying on CVI.

J. Information Protection: Chemical-terrorism Vulnerability Information (CVI)

The Advance Notice identified a category of Chemical-terrorism Vulnerability Information (CVI) and set forth rules governing the maintenance, safeguarding, and disclosure of information and records that constitute CVI.

1. General

Comment: Several commenters maintained that the proposed rule undermined enforcement, accountability, and the credibility of the program through excessive secrecy. One of these commenters thought that the proposed regulations pose a threat to existing right-to-know laws, while another stated that people might be well aware of security gaps and vulnerabilities at specific facilities, and yet would have no official channel to communicate concerns to DHS.

Response: As Congress recognized in section 550(c), protecting CVI from public disclosure is crucial to DHS's ability to ensure that chemical facilities are as secure as possible against a terrorist attack. CVI information may reveal, among other things, current vulnerabilities or other details of a chemical facility's security capabilities that

could be exploited by terrorists. In addition, limited and controlled public disclosure of CVI is essential to fostering the necessary relationship and information flow between the government and private sector. Indeed, because the chemical security regime relies to an extent in the first instance on the veracity and completeness of the information provided by chemical facilities, it is of the utmost importance that those facilities are comfortable that such information—which may include proprietary information—will not be unduly exposed to public view.

In crafting the Advance Notice, DHS attempted to balance these concerns with the desire to enhance information sharing, as appropriate. We believe that the rule adequately does this by ensuring that any entities or individuals with a "need to know," including appropriate State and local officials, will have access to the necessary CVI, while, at the same time, and consistent with congressional intent, protecting CVI from public disclosure that would undermine the government's ability to ensure the security of chemical facilities.

To the extent that this approach conflicts with existing state "right to know" or "sunshine" laws, we believe that such laws are preempted by this IFR. At this time, we do not intend to displace or otherwise affect any provisions of Federal statutes, including the Emergency Planning and Community Right to Know Act, 42 U.S.C. 11001 et seq., or section 112(r) and 114 of the Clean Air Act of 1990, as amended, 42 U.S.C. 7412(r), 7414, sections 308 and 402 of the Clean Water Act, 33 U.S.C. 1318, 1342, and section 104(e)(7) of the Comprehensive Environmental Response, Compensation, and Liability Act, 42 U.S.C. 9604.

We also believe that any potential gaps in a facility's security will be addressed

through the government's close involvement with chemical facilities as a result of this rule.

2. Disclosure of CVI

Comment: While some of the commenters found the provisions to be inadequately protective of chemical industry information, others found the disclosure rules to be too restrictive. A few commenters urged the Department to include language requiring notifications to facilities in cases of CVI disclosure to unauthorized parties. The commenters noted that a facility has a need to know if sensitive information pertaining to its site has been or might have been disclosed. A commenter, concerned over how the CVI rules may affect third-party audits of security measures and documents that may be submitted to the Department as Alternative Security Plans, requested an interpretation of DHS's approach. Taking the point further, another commenter did not believe it was in a company's best interest to provide copies of CVI to outside parties, as currently allowed under the proposed rule. The commenter would prefer the proposed rule be amended to require CVI be made readily available to authorized Department representatives only when they conduct on-site visits. One commenter encouraged the Department to adopt non-disclosure protections for verbally transmitted or obtained CVI. The commenter noted that information sharing among a covered facility and authorized individuals may require verbal communication as much as it will require written communication. To further protect against disclosure, some commenters believed that proposed § 27.400(j) should be enhanced so that it has a meaningful deterrent effect and establishes consequences that reflect the seriousness of the violation. The commenter suggested that the Department adopt administrative penalties similar to those outlined by

6 CFR § 29.9(d).

In addition, some commenters requested provisions to protect whistleblowers by stating that no criminal charges be associated with disclosing information marked as CVI in manner complying with whistleblower protections.

Response: Under § 27.400(c)(3) of the Advance Notice, "any person who . . . receives or gains access to what they know or should reasonably know constitutes CVI" is a "covered person" and therefore has a duty to protect that CVI in the manner provided in § 27.400(d). This includes the duty to promptly inform the Assistant Secretary "when a covered person becomes aware that CVI has been released to persons without a need to know. . . ." See § 27.400(d)(7). We expect that in the event DHS is so notified, it will notify the affected chemical facility.

To the extent DHS determines that it is appropriate to use third-party auditors in the future for certain chemical facilities, the auditors will have a "need to know" under § 27.400(e)(1)(i) as persons who "require[] access to specific CVI to carry out chemical security activities . . . directed by the Department." Moreover, under § 27.400(e)(3), DHS retains the discretion to require that any individuals with a need to know, including third-party auditors, complete appropriate background checks before obtaining access to CVI. We believe that these safeguards are sufficient to ensure that CVI is adequately protected from improper disclosure, even if it may be handled by third-party auditors.

Section 27.400(b) of the Advance Notice, which defines CVI, currently is ambiguous as to whether it includes information conveyed verbally as well as in written form. DHS believes that concerns over public disclosure of CVI are the same regardless of the manner in which the information is conveyed. Accordingly, we have amended this

section to read as follows: "In accordance with section 550(c) of the Department of Homeland Security Appropriations Act of 2007, the following information, whether transmitted verbally, electronically, or in written form, shall constitute CVI."

We believe that § 27.400(j) gives the Department broad latitude to craft a civil remedy sufficient to deter the unauthorized disclosure of CVI. The IFR does not provide for any criminal penalties for disclosure of CVI.

3. Scope of CVI

Comment: A number of commenters expressed concern regarding the scope of CVI. The commenters wanted the interim final rule to declare that information developed under other requirements of law or regulation cannot be designated as CVI under this program. Similarly, a commenter suggested that DHS narrow the scope of CVI by removing from the rule § 27.400(b)(9), which defines CVI to include "[a]ny other information that the Secretary, in his discretion, determines warrants the protections set forth in this part."

Response: As outlined in the Advance Notice, the Department intends CVI to include only that information developed and/or submitted pursuant to Section 550(c). Accordingly, any information resulting from other statutory regimes is not considered CVI. The Department believes, however, that the Secretary must retain the discretion provided in § 27.400(b)(9). As the Department and private sector gain more experience with the chemical security regime set forth herein, the Department may determine that other types of information, not covered in the current definition of CVI, require similar protection. Section 27.400(b)(9) is also necessary to cover any unique or novel information that the Department may deem, on a case-by-case basis, requires protection

from public disclosure.

4. Relation of CVI to Other Categories of Protected Information and FOIA

Comment: Some commenters were confused by the different categories of protected information. One commenter stated that the proposed regulations are not sufficiently clear on the relationship of CVI to SSI and other relevant methods of information protection. The commenter indicated that the interim final rule should clarify how these information protection regimes will relate to each other. A few commenters believed that the creation of the new CVI category of information protection is redundant and unnecessary given that current protections, such as SSI, are adequate options for the Department to implement the statutory restrictions. One commenter noted that the "Safeguards" classification for the Nuclear Sector seems to parallel the proposed "CVI" classification for the Chemical Sector. The commenter questioned whether the Department is considering inventing new security classifications for each of the 15 Critical Infrastructure Protection Sectors. The commenter would prefer that the Department develop a new Category of Information Classification for all 17 sectors for security-specific or security-related information that are, at a minimum, the same as those for the current "Safeguards" classification program.

Two commenters recommended that the interim final rule clarify that CVI protections would be in addition to any other applicable bases for nondisclosure of information under the Freedom of Information Act (FOIA), such as the Trade Secrets Act and its protections are for confidential business information. Another commenter noted the provision gives the Department discretion to refuse release of part of a record under FOIA that contains no CVI, when another part of the same document contains CVI. The

commenter suggests that this proposal is at odds with longstanding FOIA mandates and practice. Furthermore, the commenter noted that, if a portion of a requested record contains no CVI and is reasonably segregable from other parts of the record that do, there is no authority or justification for withholding that CVI-free portion unless some other FOIA exemption or exclusion applies.

Response: It is the Department's view that the language of Section 550(c) calls for a unique information protection regime. As stated in the preamble of the Advance Notice, in creating CVI, the Department looked to and drew on various aspects of those information protection regimes currently in existence, including, SSI, PCII and SGI. Moreover, as the Advance notice makes clear, the Department intended CVI to track the existing SSI regime in certain respects and indeed, borrowed somewhat from that regime's structure and provisions (e.g., requiring a "need to know," storage in a secure container, etc.) None of these regimes, however, is sufficient to accommodate the protections Congress called for in Section 550(c), most notably, that any information developed pursuant to Section 550(c) be treated as classified information in the course of enforcement proceedings. For this and other reasons, the Department developed CVI, which is separate and distinct from SSI, PCII, SGI or any other pre-existing information protection regime.

Section 550(c) pertains only to chemical facilities and thus this rule does not speak to the handling of other critical infrastructure sectors. 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." Absent express direction from Congress, as in Section 550(c), the Department is reluctant to create additional regimes.

In drafting the rule, the Department did not intend for its restrictions on public disclosure to displace separate and additional statutory restrictions on the public disclosure of confidential business information.

The terms and structure of Section 550 clearly preclude public disclosure of CVI. For this reason, it is the Department's view that CVI, like SSI and PCII, is exempt from FOIA disclosure under Exemption 3 of FOIA. See 5 U.S.C. 552(b)(3). Exemption 3 provides, in part, that information is exempt from disclosure by operation of another statute, provided that such statute either: "(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or (B) . . . provided that such statute refers to particular types of matters to be withheld." Id. Section 550(c) provides in relevant part that "information developed under this section, including vulnerability assessments, site security plans, and other security related information, records, and documents, shall be given protections from public disclosure consistent with similar information developed by chemical facilities subject to regulation under section 70103 of title 46 [the Maritime Transportation Security Act (MTSA)] . . . ." MTSA states that "information developed under this chapter is not required to be disclosed to the public." 46 U.S.C. 70103. Under this language, it is conceivable that the government has discretion to release information to the public. See Church of Scientology of Calif. v. U.S. Postal Serv., 633 F.2d 1327, 1330 (9th Cir. 1980). As stated in the Advance Notice, however, "information developed" under MTSA is treated as SSI and, unlike MTSA, the statute governing SSI (49 U.S.C. 114(s)) states that the government "shall prescribe

regulations *prohibiting the disclosure of information . . . .*" (Emphasis added.) This language has been interpreted as constituting the "absolute" prohibition required to invoke the exception of Subsection (A). See Chowdhury v. Northwest Airlines Corp., 226 F.R.D. 608, 611 (N.D. Cal. 2004).

To the extent that there is some ambiguity as to which statute should govern for purposes of an Exemption 3 analysis, it is our view that the SSI statute most accurately reflects Congress's intent in section 550(c) and that, therefore, CVI should be exempt from FOIA disclosure under subsection (A) of Exemption 3. Nevertheless, we need not resolve the issue at this time because it is also our view that the language of section 550(c), which provides meaningful limits on the universe of information subject to withholding, is sufficient to justify withholding CVI from FOIA disclosure under subsection (B) of Exemption 3. Cf. Fin. Corp. v. Donovan, 830 F.2d 1132, 1138 (D.C. Cir. 1989) (holding provision of Trade Secrets Act failed to qualify for subsection (B) exemption because of "exceedingly broad," "oceanic," and "encyclopedic" quality of the Act). The Department believes that it adequately expresses this conclusion in § 27.400(g)(1), which states that: "Except as otherwise provided in this section, *and notwithstanding the Freedom of Information Act (5 U.S.C. 552),* the Privacy Act (5 U.S.C. 552a), and other laws, records containing CVI are not available for public inspection or copying, nor does DHS release such records without a need to know." (Emphasis added.) Moreover, even if FOIA did apply to CVI, we believe that it would be exempt from disclosure, inter alia, as "homeland security information" under FOIA Exemption 2. See 5 U.S.C. 552(b)(2).

The commenters' concern that, if a document is portion marked to signify both CVI and non-CVI, the Department intends to withhold the entire document under FOIA, is not supported by the Advance Notice. Section 27.400(g)(2) states to the contrary that: "If a record is marked to signify both CVI and information that is not CVI, DHS, on a proper Freedom of Information Act request, may disclose the record with the CVI redacted, provided the record is not otherwise exempt under the Freedom of Information Act or Privacy Act." The use of "may" in this context was intended as permissive, assuming such disclosure is otherwise appropriate.

5. Sharing CVI with State and Local Officials, the Public, and Congress

Comment: Several comments sought greater access to CVI. Commenters stated that the Department should share CVI with State and local officials. Others noted that the definitions of "covered persons" and "need-to-know" were overly narrow and heightened their concern that the Department would not provide information to State and local officials. One commenter noted that, to the extent information is shared directly with State or local officials, DHS should enter into agreements with them to ensure that CVI is sufficiently protected. Other commenters agreed that the Department should impose strict controls for the use of any facility-specific information by States and local governments. A commenter stated that information that is provided to California local agencies may be subject to the California Public Records Act, which if true, means that CVI in California may not be protected.

A commenter recommended that the Department develop a method to share certain information with the public, such as whether a facility is in compliance with the security program, because the people who live in close proximity to a chemical facility

deserve to know. The commenter recommended the disclosure of the Letters of Approval issued upon completion of a site inspection and audit. The Letters of Approval could be stripped of any sensitive information, but still provide some assurance that facilities are complying with security requirements. Finally, other commenters stated that the interim final rule should make clear that DHS is not authorized to withhold information from either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee of Congress.

Response: Congress clearly intended that CVI would be shared with State and local officials, including law enforcement officials and first responders, in appropriate cases. Section 550(c) states that "this subsection does not prohibit the sharing of such information, as the Secretary deems appropriate, with State and local government officials possessing the necessary security clearances, including law enforcement officials and first responders, for the purpose of carrying out this section, provided that such information may not be disclosed pursuant to any State or local law." And the Department made clear in the preamble to the Advance Notice that "[t]he Secretary shall administer this Section consistent with section 550, including appropriate sharing with State and local officials, law enforcement officials, and first responders." See 71 FR 78276, 78289. Furthermore, the importance of sharing CVI with appropriate State and local officials is reflected in the structure of the rule. For example, it is expected that chemical facilities will coordinate extensively with state and local officials—including the sharing of relevant CVI—in the course of completing the SSPs required under § 27.225. It is the Department's view, therefore, that the language in the rule is sufficiently broad to accomplish this task. For example, we believe that State and local officials,

including law enforcement officials and emergency responders, fall within § 27.400(e)(1)(i)'s definition of those with a need to know because they will require access to CVI to "carry out chemical facility security activities approved, accepted, funded, recommended, or directed by the Department." Yet because many commenters have requested clarification on this point, the Department amends the § 27.400(e)(1) to read as follows: "A person, including a State or local official, has a need to know CVI in each of the following circumstances. . . . "

As stated above, to the extent any state law requires the public disclosure of information that is deemed CVI, it is the Department's view that such laws are preempted by this rule.

At this time the Department does not intend to provide a means of notifying the public about local chemical facilities. We will continue to consider this issue as the program progresses, however, and issue a subsequent notice if necessary.

This rule does not attempt to displace or create any new law concerning the Department's ability to withhold information from Congress.

6. Litigation

Comment: With respect to availability of CVI during litigation, some commenters supported the preamble statement that, in enforcement cases, the defendant and its counsel would have access to relevant CVI to enable them to prepare a full defense. Another commenter supported the Department's proposal to prohibit the disclosure of CVI in civil litigation unrelated to Section 550 enforcement. Yet another commenter stated that, according to the proposed rule, information on routine chemicals used and produced in processes would be treated as CVI, and thus disclosed in litigation

only in extraordinary circumstances. The commenter noted that, because personal injury and workers' compensation claims are the consequences of handling many toxic substances, this provision would appear to bring these actions to an absolute halt, since these cases cannot be prosecuted without precise knowledge of the toxic substances at issue. Finally, a commenter cautioned the Department to limit those provisions governing disclosure in civil or criminal litigation to the authority delegated to the Department. The commenter saw nothing in the statute delegating the authority to issue binding regulations to govern a judicial proceeding. The commenter did think it helpful for the Department to publish regulations that express its own policies and interpretations, thereby affording others guidance as to what the Department's preferred practices will be when litigation arises.

Response: As stated above, Section 550(c) requires CVI to be treated as classified information in the context of any enforcement proceedings. This novel mandate reflects the seriousness with which Congress viewed the protection of CVI from unnecessary disclosure in administrative or judicial enforcement proceedings and, by extension, any civil litigation unrelated to Section 550. The Department approach balances this concern with the need for individuals to have access to certain CVI, as appropriate, to defend themselves in enforcement proceedings.

That said, it is not clear that the type of information involved in a worker's compensation or tort claim would necessarily constitute CVI. The mere reference to a type of chemical may not readily fit into one of the categories of information under §§ 27.400(b)(1)-(9). However, even if it did, under § 27.400(i)(6), the Secretary retains the discretion to release CVI in such proceedings.

As explained in the preamble to the Advance Notice, Section 550(c) states generally that CVI shall be treated as "classified material" in the context of any enforcement proceedings. Congress did not specify, though, whether the Department should look to the rules governing classified material in civil litigation or criminal litigation. The Department chose to mirror in large part the handling of classified material in civil litigation under 18 U.S.C. 2339B. It remains the Department's view that this is a reasoned approach to effectuating Congress's intent.

7. Protection of CVI

Comment: Other comments sought technical changes to make the rule more secure or user-friendly including: prohibiting the transmission of CVI using electronic systems unless DHS is able to provide Military Grade/Quality Encryption Devices/Systems to the private sector or provide access to government locations where this equipment is available for private sector use; extending the safeguards that the CVI provisions require in proposed § 27.400(d)(1) concerning "secure container[s], such as a safe," to establishing secure databases; modifying requirements for marking every page of a CVI document with the words "CHEMICAL-TERRORISM VULNERABILITY INFORMATION" and a lengthy warning statement; allowing facilities to mark only those pages of a document containing the CVI and the warning statement only be provided once per record, with per page reference to it as needed; indicating DHS's intention to destroy, return, or permit reclassification of Top-Screen data pursuant to proposed § 27.400(k).

Response: The Department believes that the protective measures required by §§ 27.400(d) and (f) are sufficient to adequately protect CVI.

K. Preemption

Comment: Section 27.405(a) of the Advance Notice proposed to preempt State and local laws, rules, and court decisions that conflict with, hinder, pose an obstacle to, or frustrate the regulation. Several chemical companies and associations endorsed the proposed preemption of State and local regulations because they believe that national risk-based, performance standards could be undercut by specification standards imposed by the States. These commenters expressed the concern that companies with multi-state operations could be subject to a confusing array of State programs. One commenter argued that varying State regulations also provide varying levels of protection, which the commenter did not think was Congress's intent. Other commenters noted that Maritime Transportation Security Act (MTSA), which applies to facilities located on waterways, including chemical facilities, contains an express preemption provision.

An equal number of comments from advocacy groups, State agencies, and Members of Congress opposed the Department's position on preemption. These commenters cited the lack of express language in Section 550 and the legislative history to support their position that Congress did not intend to grant DHS express or implied authority to preempt State laws and regulations. A few commenters referred to a body of case law indicating a "presumption against preemption." Other commenters, including Members of Congress, suggested Congress intended to resolve the issue of preemption in future chemical facility security legislation. Commenters also urged DHS to delete § 27.405 and allow the courts to determine the preemptive effect of the Department's chemical facility regulations.

A few commenters were concerned that the language in § 27.405 was so broad that it might be construed to preempt State health, safety, and environmental regulations. Similarly, one State requested that DHS modify the final provision to avoid any inadvertent preemption of Federal, State, or local health, safety, and environmental regulations.

A few comments were directed at the appeals procedures for preemption decisions. One commenter disagreed with the lack of benchmarks that DHS would use to determine if preemption was called for and another added that the interim final rule should specify a reasonable time period for a decision to be rendered and for the decision to constitute a final administrative decision so that judicial relief could be sought. One association stated that the preemption decision process and appeals procedures did not include State government, thereby excluding the parties whose laws, rules, and public interests are most affected. The commenter proposed including a mandatory consultation process between the State and the facility before the DHS appeal, a joint hearing opportunity with the facility and State before DHS, a written decision, and State access to a judicial appeal for an adverse decision.

Response: Please see the section below entitled "Executive Order: 13132: Federalism" for a response to these comments and a discussion of preemption.

L. Implementation of the Rule

Comment: The preamble stated that DHS is considering a phased implementation of the program. Several industry commenters and a State agency supported phased implementation because they agreed that DHS should take action on the most critical facilities first. One commenter warned that problems and issues should be addressed

prior to implementation, and another commenter requested that DHS define what tiers apply to which phases. Two members of Congress asked DHS to clarify implementation for high-risk facilities beyond Phase I.

Response: The Department will immediately and quickly address the highest risk facilities. At the same time, the Department will reach out to a broader class of facilities, (numbering in the many thousands), to gather information necessary for the Department to make risk-based tiering decisions.

M. Other Issues

1. Whistleblower protection

Comment: Many commenters thought that this regulation should provide "whistleblower protection." They explained that the regulation should protect employees that provide information on a facility's security and safety from employer retaliation. Commenters suggested that workers are on the front lines, and therefore in the best position to participate in the development of Security Vulnerability Assessments and Site Security Plans. Commenters suggested that DHS create a system which would allow individuals to report vulnerabilities, shortcomings, and failures without the fear or retaliation from the company. Commenters requested that DHS change regulatory text to provide whistleblower protection to employees, with some suggesting that DHS should include the protections found in H.R. 5695 and S. 2145.

Response: Section 550 did not give DHS authority to provide whistleblower protection, and so DHS has not incorporated specific whistleblower protections into this regulation. The Department does, however, value frank information concerning security vulnerabilities. Employees with daily involvement at high-risk facilities can certainly be

a valuable source of information. In the interest of providing some mechanism for employees to alert the Department about information at their employer's chemical facility, the Department intends to establish a telephone line through which individuals can submit security concerns to the Department. The Department will provide callers with the option of remaining anonymous.

2. Inherently Safer Technology

Comment: The Department received numerous comments on the issue of inherently safer technologies (IST) options. Several commenters, including advocacy groups, unions, academics, State agencies, and other officials, strongly encouraged DHS to consider safer technologies as well as physical countermeasures. A few commenters, including members of Congress, suggested that the Department should address the use of ISTs, even though Section 550 was silent on the issue. Many of these commenters urged DHS to include provisions in the rule that would encourage chemical facilities to consider implementing safer processes and using safer chemicals as a method to improve site security through the reduction of risk. They suggested that DHS require chemical companies to analyze and report on safer technologies in their Site Security Plans. These commenters asserted that substituting safer chemicals, processes, practices, or technologies not only contributes to severity (i.e., can minimize the consequences associated with an accident at or attack on a chemical facility), but has the potential to greatly minimize the physical security costs a chemical facility would otherwise have to assume. Other commenters pointed out that ISTs are the best tools available to completely mitigate facility vulnerabilities and safeguard communities.

In contrast, other commenters rejected the use of any IST requirements. Some

argued that inherently safer technologies are an environmental construct and should not be implicitly or explicitly required for security. One association expressed concern that requirements for safer technologies could shift rather than reduce risk and/or limit the production of certain chemicals. In addition, some commenters urged DHS to avoid including any "pseudo-IST mandates" in the rule; the commenter thought that DHS had inadvertently done so.

Response: Section 550 prohibits the Department from disapproving a site security plan "based on the presence or absence of a particular security measure," including inherently safer technologies. See Section 550(a). Even so, covered chemical facilities are certainly free to consider IST options, and their use may reduce risk and regulatory burdens.

3. Delegation of Responsibility

Comment: Another commenter strongly recommended that DHS consider delegating oversight responsibility to State governments, along with appropriate levels of Federal funding to support homeland security efforts. Interested states could petition DHS, and DHS would grant delegated authority on a discretionary basis. The commenter suggested that DHS could retain oversight authority, but would delegate programmatic responsibility and commit resources to authorized States. The commenter likened the arrangement to the one that the EPA uses to handle air and water regulations and the one that the Nuclear Regulatory Commission runs with its "Agreement State" program. Another State agency commenter noted that California has promulgated a successful chemical safety program built on partnering State and local regulatory interests with chemical industry hazard mitigation activities.

Response: The Department has contemplated the issue of delegating authority to State governments, and has decided not to do so. If the Department reconsiders the issue in the future, it will provide notice any such decision.

4. Interaction with other Federal Rules and Programs

Comment: Many commenters pointed out potential overlap between this rule and other Federal agency rules. As one commenter stated, many Federal agencies have some involvement in chemical facility security, including DHS (including the U.S. Coast Guard and TSA), the Federal Bureau of Investigation (FBI), the Bureau of Alcohol, Tobacco, Firearms, & Explosives (ATF), the Departments of State, Commerce, and Transportation (including its modal administrations), EPA, and OSHA. Other commenters encouraged DHS to build upon the existing EPCRA and the Risk Management Program (RMP) regulatory programs, because of their proven records of success and the important health, safety, and environmental purposes that they serve.

One commenter noted that DOT has security plan requirements in 49 CFR Part 172, Subpart I and that several of the DHS performance standards overlap with the DOT security plan requirements. One commenter asserted that the proposal in the Advance Notice attempted to cover up knowledge of toxic dangers by potentially "gutting the worker and public right-to-know provisions" of existing Federal and State laws, including the Occupational Safety and Health Act and the Emergency Planning and Community Right-to-Know Act (EPCRA). In addition, some of these commenters were concerned that preemption and CVI classification will restrict information flow and access currently available through these Federal regulatory programs.

Several commenters expressed concern that, although DHS intends that this rule not affect other laws regulating manufacture, sale, use, and disposal of chemicals, it is unclear how the DHS security planning and enforcement can avoid impacting the environmental, occupational, trade, and other rules already regulating the same facilities. Potential conflicts also affect first responders. Since past conflicts over authority have tended to diminish program effectiveness, the commenter wonders how such conflicts can be avoided. Solutions offered by commenters include a more explicit statement on conflict resolution in the final rules, an inter-agency coordination process to resolve conflicts, or memoranda of agreement with agencies having concurrent authority.

Response: The Department is aware that potential overlap exists between this rule and existing Federal rules and programs. In the Advance Notice, the Department acknowledged that overlap and included an extensive discussion of existing and proposed Federal programs that are related to chemical security. See § I of the Advance Notice, "Brief History of Federal Pre-Existing Chemical Security Tools and Programs."

Section 550 provides that "[n]othing in this section shall be construed to supersede, amend, alter, or affect any Federal law that regulates the manufacture, distribution in commerce, use, sale, other treatment, or disposal of chemical substances or mixtures." In the Advance Notice, after acknowledging that the ATF regulates the purchase, possession, storage, and transportation of explosives, the Department indicated that it did not intend for these regulations to interfere with ATF's current authorities. See 71 FR 78276, 78290. Likewise, the Department does not intend for these regulations to impede the authorities of other Federal agencies. With respect to this regulatory program, DHS will work closely with the Department of Energy, EPA, OSHA, ATF and

other federal agencies. Where there is concurrent jurisdiction, the Department will work closely with other Federal agencies to ensure that regulated facilities can comply with applicable regulations while minimizing any duplication. As the program develops, the Department will consider the necessity of various formalized arrangements, such as an inter-agency coordination process, to resolve jurisdictional questions or conflicts.

5. Third-Party Actions

Comment: Several commenters supported the Advance Notice discussion of the statutory prohibition against third party actions to enforce any provision of the chemical security rules. See § 27.410 and Section 550(d). A State commenter wrote that the prohibition might be construed to prevent State actions against the Department to enforce the regulations, a position that the commenter believed to be contrary to congressional intent. The commenter agreed that the statutory language would bar a State from taking enforcement action against an owner or operator for violation of these regulations, but it saw no support in the statute to bar State action against the Department (or other non-owners or non-operators). According to the commenter, this interpretation exceeds the scope of Section 550 and is therefore an unnecessary limitation on private rights of action. Commenters asserted that a plain reading of Section 550 indicates that Congress limited judicial review in only two ways: (1) by prohibiting Section 550 from being asserted as a jurisdictional basis for a cause of action; and (2) by providing that only the Secretary of Homeland Security has the right to bring enforcement actions against "owners and operators." The commenters said they do not believe that Congress intended to prohibit other statutory causes of actions (such as review pursuant to the Administrative Procedure Act).

Members of Congress also challenged the broad scope of DHS's position on third-party suits, because it would block basic challenges to DHS under the Administrative Procedure Act. The commenters believed that § 27.410(a) was an unnecessary limitation on private rights of action. One Member of Congress explained that Congress intended to limit the provision to citizen suits against chemical facilities for failure to comply with the Department's chemical security rules.

One commenter strongly supported the Department's discussion of the prohibition of private rights of action to enforce the provisions of Section 550. The commenter believed that the availability of enforcement actions should be limited to avoid unnecessary and potentially frivolous lawsuits that attempt to enforce chemical facility security requirements that are outside the reach of the government's authority.

Some commenters supported the DHS provision because they believed that third party actions should be limited and that the Department should have the sole discretion of when and how to enforce these regulations. One commenter stated that neither DHS nor regulated chemical facilities should be distracted from their purpose of minimizing the possibility of a catastrophic terrorist incident by concerns about how their actions implementing Section 550 might be used in private tort litigation. One industry organization supported § 27.410(b), which allows a chemical facility to petition DHS to provide "the Department's view in any litigation involving any issues or matters regarding this Part." The commenter noted that DHS is in a unique position, in light of its Section 550 authorities and expertise, to provide its views regarding a chemical facility's security efforts.

A labor union expressed concern that § 27.410(a) grants immunity to chemical facilities from actions by third parties to enforce any provisions of the rule. The labor union thought that it may act as an open invitation to chemical facilities to disregard provisions in the rules or in security plans that are meant to protect maritime activities from unduly burdensome or improper application of security procedures. The labor union explained that "[w]here damages are incurred by maritime-related businesses or mariners as a result of improper action of chemical facilities under color of enforcing their security plans, the injured parties should not be denied the normal recourse of the U.S. legal system."

Response: In § 27.410 of the Advance Notice, the Department set out two principles: (1) the chemical security regulations did not on their own terms create any additional rights of action for any person other than the Secretary; and (2) relevant parties may seek a statement from the Department of its views in any litigation involving the chemical security regulatory program. The Department has decided to adopt these provisions as proposed in the Advance Notice.

In the preamble to the Advance Notice, the Department also stated its view that Section 550(d) prohibits any party other than the Secretary from enforcing the provisions of Section 550. The Department also stated its view that Section 550(d) prohibits actions brought to compel the Department to take a specific action to enforce Section 550. Although the Department does not find it necessary to codify these views in the Code of Federal Regulations, they remain the views of the Department after considering the comments received. In Section 550(d), Congress provided in clear terms its intent to prevent parties other than the Secretary from making enforcement decisions under

Section 550. This intent would be thwarted if parties could seek indirectly to have particular enforcement measures taken by bringing suit against the Department. Such suits would also pose difficulties involving the information protections of Section 550 and its implementing regulations. In short, the terms and structure of Section 550 provide the Secretary with critical discretion in implementing the chemical security program. It would be inappropriate to curtail that discretion through lawsuits. See generally Norton v. Southern Utah Wilderness Alliance, 542 U.S. 55 (2004).

6. Judicial Review

Comment: Several commenters, including Members of Congress, urged DHS to incorporate the right to judicial review in the interim final rule and clarify the judicial remedies available. One commenter mentioned that the right to judicial review was expressly stated in prior legislative proposals. Another commenter believed that the District Courts have jurisdiction to consider whether a facility presents a "high level of security risk." Other commenters discussed judicial review in the context of preemption, urging the Department to provide facilities with the opportunity for judicial review of Departmental decisions pursuant to § 27.405. Finally, one commenter recommended that the rule provide that if the adjudicating official fails to reach a decision within the timeframes provided by the proposed rule, then the administrative review process is deemed completed and all administrative remedies exhausted, so as to afford the facility the ability to challenge the Department's decision in a District Court.

Response: The Department does not have authority to create jurisdiction in the district courts for review of Department decisions. Jurisdiction is created by provisions of law other than these regulations. Nor does the Department have authority to create

specific judicial remedies through rulemaking. Decision-making authority with respect to preemption is discussed below in the portion of this preamble related to Federalism. As discussed there, courts have the ability in appropriate contexts to review the Department's opinions as they relate to preemption. This interim final rule does not augment the administrative law default principles that govern appropriate action if the Department does not make decisions in the timeframes specified in this interim final rule.

7. Guidance and Technical Assistance

Comment: Some industry commenters noted that guidance, information, and education were essential for the success of the program. A chemical company commented that facilities should have the opportunity to review and comment on any guidance provided to them by DHS. Several industry associations made the same comment and stated the need for guidance to provide direction and advice but not to become either enforceable or limiting in the security measures that a facility may employ.

One commenter suggested that there be sufficient time to respond to the guidance prior to developing a security plan. Commenters suggested that DHS draft guidance on aspects of the regulation and that such guidance be as detailed and specific as possible.

One commenter believed that, while agency guidance is procedurally easier to issue because agencies typically issue it without notice and comment, due process, or other protections afforded by rulemaking under the Administrative Procedure Act, this "pseudo-rulemaking" can be referenced in enforcement actions, imposing cost burdens, or creating other compliance liabilities. Another commenter appreciated the fact that the guidance would specify the security measures that facilities could take to meet the proposed standards while not mandating any particular measures that facilities should

use. Commenters recommended that DHS follow the OMB Bulletin entitled "Agency Good Guidance Practices," which establishes policies and procedures for the development, issuance, and use of significant guidance documents by Executive Branch departments and agencies.

Response: DHS believes that guidance will play an important role in this regulatory program. The Department's guidance will provide examples of specific measures that facilities may use to address the performance standards in the rule. Because this rule is based on performance standards and not on prescriptive measures, guidance is particularly important. The guidance will aid in informing the regulated community of ways to satisfy the performance standards without imposing additional requirements not found in these regulations.

The Department will designate the guidance document as CVI. The guidance document will contain specific anti-terrorism measures designed to mitigate or prevent terrorist attacks, as well as other sensitive information. This type of information is not appropriate for public disclosure under Section 550 and the regulations issued hereunder.

With respect to comments regarding OMB's Bulletin on Agency Good Guidance Practices, the Department notes that it will apply the Bulletin as appropriate.

Comment: The availability of technical assistance to facilities not placed in the top tier was requested by an industry association.

Response: Technical assistance will be available for all covered facilities as resources permit. Section 27.120 establishes requirements for a Coordinating Official who will provide guidance to facilities in all tiers, as necessary and to the extent that resources permit.

8. Miscellaneous Comments

Comment: One commenter recommended that DHS engage and work with Congress to enact a more comprehensive and meaningful chemical security law as soon as possible, and under no circumstances beyond the three year expiration of interim authority.

Response: The Department has aggressively sought this authority, and on October 4, 2006, Congress provided that authority. The Department will continue to work with Congress on chemical security matters.

Comment: One commenter supported the position that continued funding of this program would, in effect, reauthorize the program beyond the three years noted in the statute and that DHS may amend the interim final rule if necessary. Another commenter did not support this position and stated that the statute was clear that the regulatory authority expires after three years. That commenter also urged the Department to engage in notice and comment rulemaking for any future modifications to the interim final rule.

Response: The Department will, to the extent required by law, engage in notice and comment rulemaking in the event that changes are made to this interim final rule.

Comment: Commenters suggested a process by which facilities can exit the program if they make sufficient changes to their operations. In addition, a chemical company and an industry association questioned how the results from vulnerability assessments could be used to allow a facility to exit the program.

Response: To address the issue of exiting the program, the Department added § 27.120(d). It provides that covered facilities may request a consultation with the Department if their facility, processes, or types or quantities of chemicals change in such

a way that they believe their obligations under this part may be impacted. For a discussion of this provision, see § II(B) above.

Comment: Various commenters raised issues related to data security, specifically in the context of the Department's web-based CSAT applications. One commenter thought that DHS should be able to provide Military Grade/Quality Encryption Devices/Systems for the private sector to use to submit information. Until that time, the commenter requested that DHS receive information only in paper form or discs produced on stand-alone computers.

Response: DHS recognizes the data security issues that commenters have raised. DHS realizes that there is a risk, both on the sending of information and the receiving of information, when transmitting data over the Internet. DHS has weighed the risk to the data collection approach against the risk of collecting the data through paper submissions and concluded that the web-based approach was the best.

DHS is concerned about data security and has taken a number of steps to protect both the data that will be collected through the CSAT program and the process of collection. The security of the data has been the system designers' number one priority. The site that the Department will use to collect submissions is equipped with hardware encryption that requires Transport Layer Security (TLS), as mandated by the latest Federal Information Processing Standard (FIPS). The encryption devices have full Common Criteria Evaluation and Validation Scheme (CCEVS) certifications. CCEVS is the implementation of the partnership between the National Security Agency and the National Institute of Standards (NIST) to certify security hardware and software.

Upon completing any part of the CSAT (whether the Top-Screen, Security Vulnerability Assessment, or Site Security Plan), the facility will click a "submit" button, which calls a routine to encrypt the data on the server using a one way key. Properly-executed public key encrypted data is very secure, and the implementation that DHS has used complies with the NIST 800-57 requirements for security. The key to decrypt the data does not exist outside of facilities that are isolated from the public internet. The key is connected only through a dedicated, restricted, government network that cannot connect to the public internet. Once a facility submits a Top-Screen (or SVA or SSP), the data is no longer available unencrypted.

Comment: A few commenters indicated that the Advance Notice lacked meaningful worker involvement. According to some of the commenters, the rule does not ensure meaningful front line worker and union participation during risk assessments, during the development of the Site Security Plans, in the inspection process, or as part of ongoing consideration of safety and security concerns. One commenter felt that this omission occurred despite the fact that it is the front line employee whose life is on the line first if there is a catastrophic release.

Response: There is nothing in the rule that prohibits chemical facilities from involving employees in their security efforts. Many facilities may find it beneficial to include employees in their respective efforts to comply with this regulation (e.g., identifying security vulnerabilities, developing Site Security Plans). However, the Department is not mandating participation by any particular type of employee, and the Department does not think it is wise to specify any employees that must be involved. The Department will leave those decisions to facilities, as they will best understand the

types and functions of employees at their facility and the extent to which any given type of employee may be able to contribute.

Comment: A commenter noted that a strong enforcement program is essential.

Response: The Department agrees with the commenter and will vigorously enforce these regulations.

Comment: A few commenters sought immediate phased-in implementation of a national re-routing and a ban on toxic by inhalation (TIH) storage wherever feasible. Although the commenters stated that re-routing is the first and fastest step in eliminating catastrophic vulnerabilities in the chemical sector, the commenters thought it should ideally be done in tandem with the use of safe technology, which could in turn eliminate ultra-hazardous substances in our rail system.

Response: These comments are beyond the scope of this rulemaking, which addresses chemical facility anti-terrorism standards. However, DHS points out that there are current DHS and other Federal initiatives to address materials that are toxic by inhalation. On December 21, 2006, TSA issued a Notice of Proposed Rulemaking on Rail Transportation Security. See 71 FR 76852. The rule applies, in part, to tank cars containing materials that are poisonous by inhalation (PIH) as defined in 49 CFR § 171.8. (Note that the PIH is synonymous with TIH). See proposed 49 CFR § 1580.100(b). Also, on December 21, 2006, one of the Department of Transportation's modal administrations, the Pipelines and Hazardous Materials Administration (PHMSA), issued a Notice of Proposed Rulemaking titled "Hazardous Materials: Enhancing Rail Transportation Safety and Security for Hazardous Material Shipments." See 71 FR 76834. PHMSA's proposed regulation would include requirements for rail carriers to use

data to analyze safety and security risks along rail transportation routes where certain hazardous materials (including PIH materials) are used.

Comment: Some commenters raised questions regarding specific funding for programs such as the BZPP Webcam Pilot Program.

Response: Those comments are beyond of the scope of this rulemaking, which addresses chemical facility anti-terrorism standards.

N. Regulatory Evaluation

Comment: Commenters believe that DHS has underestimated this cost to the chemical sector and that DHS should consider other costs beyond capital costs, such as additional physical security.

Response: In the Advance Notice, DHS did not attempt to estimate the full cost of complying with the regulation. Instead, DHS placed in the docket a stand-alone document titled "Capital Cost Information for Public Comment," which provides specific cost estimates for a potential suite of capital security investments, such as fences and perimeter lighting. DHS fully understands that, in addition to capital costs, facilities may also incur non-capital costs, including the costs of additional personnel (e.g., security guards) and the costs of preparing assessments and plans. The costs that DHS has estimated for compliance with the interim final rule do indeed include both the capital costs and non-capital costs.

DHS also notes that while a few commenters thought the costs DHS presented were too low, commenters did not generally provide specific information regarding which costs may have been too low or additional information that would have assisted the Department in reconsidering the costs presented with the Advance Notice. Consequently,

while DHS did re-evaluate the costs presented with the Advance Notice in response to these comments, DHS believes that the costs presented in the Advance Notice are reasonable approximations, and they remain unchanged in the interim final rule.

Some commenters indicated that cost recovery for implementation can be difficult under certain government contracts. Such comments are outside of the scope of this rulemaking.

Comment: Commenters also expressed concern that the high costs will give an unfair advantage to larger companies, because these associated costs will be harder for smaller companies (like local farmers) to absorb.

Response: The Department notes, in general, that it may be more difficult for smaller companies to absorb increased costs than larger companies. However, the security measures required by this interim final rule are not "command and control" type measures. Instead, they are risk-based performance measures that will allow a high degree of flexibility for small entities that own high-risk chemical facilities. These risk-based performance measures will allow high-risk chemical facilities to tailor a specific regulatory compliance regime that could minimize the compliance costs to their respective facilities. DHS also notes that certain chemical facilities have already voluntarily spent a significant amount of financial resources to increase their security. This interim final rule, by establishing a baseline level of security across tiers, will serve to minimize any competitive advantage that may be currently enjoyed by those companies that are under-investing in security.

Comment: One commenter noted that in order to quantify the benefits of the rule, DHS must make assumptions about the threats to the public, which injects uncertainty into the calculation of actual benefits.

Response: The Department agrees that it is difficult to quantify the "actual benefits" of this interim final rule. DHS has included a qualitative discussion of the benefits of this rule in the regulatory analysis of Executive Order 12886, which is located in Section IV of the preamble to this rule.

Comment: Commenters noted that the idea of a model facility is indeed a good proposal but worried that there is insufficient time to implement the changes this proposal would entail.

Response: DHS agrees that the idea of model facilities is a good proposal. The cost estimate of the interim final rule is based on the concept of the "model facility" as it was used by the Coast Guard to estimate the cost of their Maritime Transportation Security Act of 2002 Facility Security final rule. See 68 FR 60515 (Oct. 22, 2003).

Comment: The Small Business Administration (SBA), Office of Advocacy, commented that DHS should prepare an Initial Regulatory Flexibility Analysis (IRFA) under the Regulatory Flexibility Act (RFA), 5 U.S.C. 603, after issuing the interim final rule or if DHS makes subsequent changes to the rule once it is promulgated. SBA explained that the RFA process is an extremely valuable tool for agencies to use when assessing the impact of a rule on small businesses and other small entities.

Response: The RFA mandates that an agency conduct an analysis when an agency is required to publish a notice of proposed rulemaking. See 5 U.S.C. 603(a). In this case, the Department is not required to publish a notice of proposed rulemaking: By

directing the Secretary to issue "interim final regulations", Congress authorized the Secretary to proceed without the traditional notice-and-comment required by the Administrative Procedure Act. See 71 FR 78276, 78277, and 78292 (Dec. 28, 2006).

DHS did, however, consider the impacts of this rule on small entities. The Regulatory Assessment, which is available in the public docket, contains our analysis of the impacts of this rule on small entities. After consideration of the percentage of small entities that may have to comply with the risk-based performance standards required by this rule and the compliance costs explained in the Regulatory Assessment, we have determined that this rule may have a significant economic impact on a substantial number of small entities. See "Regulatory Flexibility Act" section below.

IV. Regulatory Analyses

A. Executive Order 12866: Regulatory Planning and Review

This rule is considered to be an economically significant regulatory action under Executive Order 12866, because it will result in the expenditure of over $100 million in any one year. Accordingly, this rule has been reviewed by the Office of Management and Budget (OMB). A Regulatory Assessment which more thoroughly explains the assumptions used to generate the cost of this interim final rule is available in the docket as indicated under **ADDRESSES**. A summary of the Regulatory Assessment follows:

Cost Assessment Summary

Section 550 requires the Secretary of Homeland Security to promulgate "interim final regulations establishing risk-based performance standards for security of chemical facilities * * *." He must do so "[n]o later than six months" from the date of enactment of this new authority, *i.e.* by April 4, 2007. Consequently, the methodology chosen to

analyze the cost of the interim final rule was chosen with the six month congressional deadline in mind. In order to quickly analyze the cost of the interim final rule, DHS relied on readily available information and drew upon the knowledge of professionals employed by DHS who have extensive knowledge of the chemical industry. In addition, on December 28, 2006, DHS published an Advance Notice, which outlined our costing methodology and also placed in the docket our estimates of capital costs for potential security investments in order to seek meaningful public comment.

We have reviewed the methodology used by the U.S. Coast Guard to analyze the cost of the MTSA Facility Security final rule at 68 FR 60515 (Oct. 22, 2003), and, due to the similarities between the MTSA Facility final rule and this interim final rule, we believe that this methodology has merit and should be used in this rulemaking. The MTSA Facility Security final rule estimated the cost of performance standards on several thousand unique facilities. Similarly, the interim final rule will estimate the costs of risk-based performance standards to several thousand unique facilities. The Coast Guard found it impractical to attempt to estimate compliance costs for each individual facility and instead developed costs based on 16 "model facilities." Each of the several thousand facilities was placed into one of the 16 different subgroups for which compliance costs were then estimated. Once the compliance costs for the 16 "model facilities" were calculated, estimating the cost of the regulation was relatively straightforward.

As this regulation is not a "command and control" regulation, owners and/or operators will have considerable flexibility in how they choose to comply with its requirements. As owners and/or operators will have discretion on how to best meet the risk-based performance objectives, the cost assessment makes broad assumptions

regarding the percentage of facilities that will choose to implement or continue certain security measures and the costs of those security measures. For example, many facility owners and/or operators will choose such measures as building fences, enhancing perimeter lighting, and hiring additional security guards in order to comply with the risk-based performance standards. In order to estimate the cost of the interim final regulation, we made assumptions regarding the specific percentage of facilities that will choose to implement certain security measures, such as fences and perimeter lighting.

We expect that chemical facility owners and/or operators will take full advantage of the flexibility that these risk-based performance standards will provide and will conduct facility-specific and company-specific analyses to determine the most cost-effective method to comply with the requirements of this interim final regulation. As a result of these internal analyses, facilities are likely to identify various means of meeting the risk-based performance standards applicable to their facility and tier. It is possible that some percentage of facilities will find the most-cost effective method to comply with the requirements will be to implement business and related production, processing or equipment changes such as to no longer make certain chemicals or to change their process to use a less concentrated or less hazardous form of a listed chemical. Such process changes, however, are very facility-, business- and process-specific. Those that involve changes in chemistry or processes may take several years of design, testing and re-permitting before they can become operational. Others may be easily and immediately implemented. However, because process changes are so facility- and business-specific, DHS has no way of estimating how many facilities may ultimately implement such measures for the purpose of estimating compliance costs. Consequently, DHS is basing

its estimate of compliance costs on commonly used security measures that are broadly applicable to a wide range of high risk chemical facilities, such as the purchase of fences, the purchase of perimeter lighting, and the employment of security guards.

For the purposes of good practices or regulations promulgated by other Federal or State agencies, many chemical facility owners and/or operators have already spent a substantial amount of money and resources to upgrade and improve security. The costs shown below do not include the costs of security measures already implemented to enhance security. The costs shown here are intended to represent the marginal cost incurred by owner and/or operators as a result of the interim final rule.

DHS's preliminary estimate of the number of high risk chemical facilities that will be covered by the risk-based performance measures required by the interim final rule ranges from 1,500 to 6,500 chemical facilities. It is important to stress that this estimate is simply DHS's best guess based on currently available information. Within this range of 1,500 to 6,500 potentially covered chemical facilities, DHS is estimating 5,000 facilities as its best guess of covered facilities for the purpose of generating the cost estimate required by Executive Order 12866.

Using the point estimate of 5,000 facilities, the estimated present value cost of this interim final rule is $3.6 billion dollars over the period 2006-2009[2] (7 percent discount rate). For the purposes of illustration, we also have calculated the cost of the interim final rule over the ten year period 2006-2015. Over the period 2006-2015, DHS

[2] Section 550(b) of the Act states: "Interim regulations issued under this section shall apply until the effective date of interim or final regulations promulgated under other laws that establish requirements and standards referred to in subsection (a) and expressly supersede this section: *Provided*, That the authority provided by this section shall terminate three years after the date of enactment of this Act."

estimates the present value cost of this interim final rule would be $8.5 billion assuming 5,000 covered facilities.

Benefits Assessment

This interim final rule allows DHS to implement Section 550 of the Homeland Security Appropriations Act of 2007. The first sentence of Section 550 mandates the Secretary to issue interim final regulations establishing risk-based performance standards requiring the performance of vulnerability assessments and the development and implementation of site security plans. Section 550 establishes the parameters of the Federal government's first regulatory program to secure chemical facilities against possible terrorist attack.

The threat of a terrorist attack against high-risk chemical facilities is real. However, due to the economics of externalities, the free market may not provide adequate incentives for chemical facilities to make a socially optimal investment in the full range of measures that would reduce the probability of a successful terrorist attack. Externalities are a cost or benefit from an economic transaction experienced by parties "external" to the transaction. In the case of chemical facilities, since the consequences of an attack or other security incident may be significantly larger than what would be suffered by the owner of the facility itself, the private market may not generally provide the incentive for profit-maximizing firms to unilaterally spend the socially optimal amount of resources to prevent or mitigate a terrorist attack. Since companies nevertheless will likely suffer serious consequences in the case of a terrorist attack, many certainly have invested significant resources in implementing security measures, and this analysis recognizes those resource expenditures. In a competitive marketplace, however,

a firm will not normally choose to make some additional investment in security over their privately optimal amount, since they would consequently be choosing to increase its cost of production and would be at a disadvantage when competing with companies that have chosen not to make a similar investment in security. As this interim final rule will require high-risk chemical facilities to be held to the same risk-based performance standards according to their risk-based tier, the competitive advantage that may be currently enjoyed by those companies that are under-investing in security measures would be expected to disappear.

Need for Increased Security at High-Risk Chemical Facilities

There is much publicly-available information that indicates an attack on a chemical facility is a credible threat with dire consequences:

- According to the Government Accountability Office, experts agree that the Nation's chemical facilities present an attractive target for terrorists who are intent on causing massive damage. Many facilities house toxic chemicals that could become airborne and drift to surrounding communities if released or could be stolen and used to create a weapon capable of causing harm. Terrorist attacks involving the theft or release of certain chemicals could have a significant impact on the health and safety of millions of Americans. The disaster at Bhopal, India in 1984, when methyl isocyanate gas—a highly toxic chemical—leaked from a tank, reportedly killing about 3,800 people and injuring anywhere from 150,000 to 600,000 others, illustrates the potential threat to public health from a chemical release.[3]

[3] GAO, *Homeland Security: Federal and Industry Efforts Are Addressing Security Issues at Chemical Facilities, but Additional Action is Needed*, GAO-05-631T (Washington, D.C.: April 2005).

- The Department of Justice has concluded that the risk of terrorists attempting in the foreseeable future to cause an industrial chemical release is both real and credible. Terrorists or other criminals are likely to view the potential of a chemical release from an industrial facility as a relatively attractive means to cause mass casualties to the populace and/or large scale damage to property. DOJ notes that there have been successful efforts by foreign militaries and certain terrorist groups indigenous to other countries to cause releases from industrial facilities using bombs. Those efforts have in effect converted the facilities into makeshift WMD. Some of these releases have inflicted damage on the surrounding communities. Moreover, the evacuations that were triggered by the attempted and successful releases of industrial chemicals produced panic and disruption among the targeted population. These are precisely the goals of a terrorist.[4]

- In April 27, 2005, testimony before the Senate Committee on Homeland Security and Governmental Affairs regarding the vulnerability of America to a chemical attack, a Brookings Institution Visiting Fellow testified. The testimony stated that "of all the various remaining civilian vulnerabilities in America today, one stands alone as uniquely deadly, pervasive, and susceptible to a terrorist attack: toxic-inhalation-hazard (TIH) industrial chemicals, such as chlorine, ammonia, phosgene, methyl bromide, hydrochloric and various other acids." In addition, the testimony indicated, "the casualty potential of a terrorist attack against a large TIH chemical container near a population center is comparable to that of a fully successful terrorist employment of an improvised nuclear device or effective biological weapon. The key difference is that TIH chemical

[4] *Department of Justice Assessment of the Increased Risk of Terrorist or Other Criminal Activity Associated With Posting Off-Site Consequence Analysis Information on the Internet*, April 18, 2000.

containers are substantially easier to attack than improvised nuclear devices or effective biological weapons are to acquire or fabricate."[5]

- In April 27, 2005, testimony before the Senate Committee on Homeland Security and Governmental Affairs regarding the vulnerability of America to a chemical attack, a Senior Fellow for National Security Studies at the Council on Foreign Relations testified. The testimony stated "Of the carefully selected potential targets that al Qaeda or its imitators might seek to attack, the chemical industry should be at the top of the list. There are hundreds of chemical facilities within the United States that represent the military equivalent of a poorly guarded arsenal of weapons of mass destruction."[6]

- A recent Congressional Research Service Report discussed trends in chemical terrorism and discussed evidence that U.S. chemical facilities may be used by terrorists to gain access to chemicals. One of the 1993 World Trade Center bombers, Nidal Ayyad, became a naturalized U.S. citizen and worked as a chemical engineer in the chemical industry, from which he used company stationery to order chemical ingredients to make the bomb."[7]

- Information contained in the Congressional Record states that U.S. chemical trade publications were found in one of the caves where Osama bin Laden had hidden.[8]

Qualitative Benefits of the Risk-Based Performance Standards

[5] Statement of Richard A. Falkenrath, Visiting Fellow, The Brookings Institution, before the United States Committee on Homeland Security and Governmental Affairs (April 27, 2005).
[6] Statement of Stephen E. Flynn, PhD, Jeane J. Kirkpatrick Senior Fellow for National Security Studies, Council on Foreign Relations, before the United States Committee on Homeland Security and Governmental Affairs (April 27, 2005).
[7] CRS Report for Congress, *Chemical Facility Security*, Updated August 2, 2006.
[8] Bond, Christopher. Statement on S.2579. *Congressional Record*, Daily Edition, June 5, 2002, p.S5044.

As explained previously, Section 550 requires the Secretary of Homeland Security to promulgate ‘‘interim final regulations establishing risk-based performance standards for security of chemical facilities * * *.” Section 27.230 establishes these standards. Below is a discussion of the qualitative benefits of these risk-based performance standards:

- By securing and monitoring the perimeter of the facility, site personnel are better able to detect, delay, and respond to individuals or groups who seek unauthorized access to the site or its restricted areas. A well-secured perimeter deters intruders from seeking to gain access. By limiting access through control points, the facility can more easily and effectively control who enters and leaves the site. Additionally, securing and monitoring restricted areas or potentially critical targets within the facility reduces the likelihood of theft of chemicals because adversaries risk observation arriving and leaving the premises. Control of gates by guards or observation of the perimeter allows facility personnel to know who is entering and leaving the site and in what vehicles. Access control points permit the facility to check persons and vehicles seeking entrance to the site and confirm their legitimate business.

- Controlling access to the site including the screening and/or inspection of individuals and vehicles as they enter and exit the facility serves to deter and detect unauthorized introduction or removal of substances and devices that may cause a dangerous chemical reaction, explosion, or other release to harm facility personnel or the surrounding community. A regular system of identification checks will help guards and other facility personnel recognize those personnel authorized to be on the site and identify those individuals who should not be granted access.

- Deterring vehicles from entering the facility or restricted access areas will reduce the likelihood that an adversary will detonate a vehicle-borne improvised explosive device inside the facility. Appropriate methods of deterring vehicles from unauthorized entry provide additional time for local law enforcement response or otherwise delay or prevent the vehicle from entering the site to cause harm.

- Securing and monitoring the shipping and receiving of hazardous chemicals will improve inventory control, product stewardship and security against theft, diversion and tampering. In addition, improved inventory control and control of transportation containers on site decreases the likelihood that a foreign substance could be introduced into feedstock, incidental chemicals, or products leaving the site that could later react with the chemical to cause a significant on- or off-site reaction to damage process equipment or cause a release of a hazardous material to harm onsite personnel or the community.

- Deterring the theft or possible diversion of potentially hazardous chemicals will prevent loss of chemicals from the site. Such measures provide security benefits as well as improving inventory controls especially for chemicals that can be used directly as a chemical weapon or can be used to produce such a weapon.

- Deterring insider sabotage prevents the facility's own property and activities from being used by a potential terrorist against the facility. Examining the background of employees or contractors who may be planning acts of sabotage assists in preventing an *in situ* release of hazardous chemicals, damage to process units manufacturing chemicals or tampering with chemicals that could cause an offsite impact. Ascertaining that visitors

and contractors have legitimate business onsite and are escorted when necessary increases the control of the site in general and reduces the likelihood of sabotage or theft.

- The deterrence of cyber sabotage will benefit the facility by preventing unauthorized onsite or remote access to critical process controls, site security, business systems, or SCADA systems (if significant consequences can be generated by the manipulation of the process controls/ systems). Appropriate controls will allow the detection of unauthorized access and unauthorized modification of information (hacking).

- Developing and exercising an emergency plan to respond to security incidents internally and with local law enforcement and first responders (i.e., emergency medical technicians (EMTs), fire, police) benefits the facility by preparing it to take quick and decisive action in the event of an attack or other breach of security. Establishing relationships with local law enforcement improves responder understanding of the layout and of hazards associated with the facility and strengthens relationships with the community.

- Maintaining effective monitoring, communications and warning systems allows the facility to notify internal personnel and local responders in a timely manner about security incidents. Regular tests, repairs and improvements to the warning and communications system increase the reliability of such systems and will improve response time.

- When the facility provides proper security training, exercises and drills, facility personnel are better able to respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders. Well trained personnel who practice how to react can more effectively detect and delay intruders and provide

increased measures of deterrence against unauthorized acts. Establishing relationships with local law enforcement improves responder understanding of the layout and hazard associated with the facility and strengthens relationships with the community.

- The ability to escalate the levels of security measures for periods of elevated threat will provide the facility with the capacity to increase security measures to better protect against known increased threats or generalized increased threat levels declared by the federal government. By maintaining the ability to increase security measures, the facility does not have to expend time and resources on more robust security measures unless and until warranted.

- A facility addressing specific threats, vulnerabilities or risks identified by the Assistant Secretary will decrease the likelihood of a successful attack on its facility, personnel, products or community. Any additional performance standards specified by the Secretary will increase the facilities ability to deter, detect, delay and respond to specific and general threats against its security.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA) mandates that an agency conduct an RFA analysis when an agency is required to publish a notice of proposed rulemaking. See 5 U.S.C. 603(a). An RFA analysis, however, is not required when an agency is not required to publish a notice of proposed rulemaking, as is the case here. By directing the Secretary to issue "interim final regulations" Congress authorized the Secretary to proceed without the traditional notice-and-comment required by the Administrative Procedure Act. See 71 FR 78276, 78277, and 78292.

Even though a Regulatory Flexibility Analysis is not required for this rule, DHS did consider the impacts of this rule on small entities. The Regulatory Assessment, which is available in the public docket, contains this analysis of the impacts of this rule on small entities. A portion of the analysis is summarized below.

At this time, DHS's preliminary estimate of the number of high risk chemical facilities that will be covered by the risk-based performance measures required by the rule ranges from 1,500 to 6,500. This estimate is based on currently available information. After chemical facilities with certain risk profiles complete the Top-Screen, DHS will have a better understanding of how many and which specific chemical facilities will be deemed to be "high-risk" for the purposes of the rule. Also, in meeting the risk-based performance standards required by this rule, facilities will have a large degree of flexibility in choosing specific security enhancements. We expect that chemical facility owners and/or operators will use this flexibility to minimize the cost of this rule to their operations. These uncertainties make it very difficult to estimate the extent of the economic impact of this rule on small entities.

Even so, strictly for the purposes of analyzing the impact of this rule on small entities, DHS has selected from the EPA RMP database a sample of 350 facilities that *may* be required to comply with the risk-based performance standards required by the rule. We researched these 350 facilities using *Reference USA* and *LexisNexis* and found detailed information (i.e., annual revenue, number of employees, and parent company information) for 326 (93%) of them. Of the 326 facilities for which we were able to find detailed information, our analysis of the data indicates that 118 (36%) fit the Small Business Administration's definition of a small entity. If we assume that the 24

companies for which we could find no information are also small entities, the percentage of these facilities which are owned by small entities could be 41 percent. Table 1 below provides revenue ranges of the118 small entities.

Table 1. Percentage of Small Entities by Revenue

Revenue	Number of Small Entities	Percent of Small Entities
$0 - $999,999	11	9.3%
$1,000,000 - $4,999,999	14	11.9%
$5,000,000 - $9,999,999	12	10.2%
$10,000,000 - $19,999,999	15	12.7%
$20,000,000 - $49,999,999	23	19.5%
$50,000,000 - $99,999,999	9	7.6%
$100,000,000 - $999,999,999	31	26.3%
> $1Billion	3	2.5%
Total	**118**	**100.0%**

After consideration of the percentage of small entities that may have to comply with the risk-based performance standards required by this rule and the compliance costs explained in the Regulatory Assessment, we have determined that this rule may have a significant economic impact on a substantial number of small entities.

C. Executive Order 13132: Federalism

1. Background

Executive Order 13132 requires DHS to develop a process to ensure "meaningful and timely input by State and local officials in the development of regulatory policies that have federalism implications." Between the publication of the Advance Notice and this Interim Final Rule, the Department has complied with this instruction in two ways. The Department specifically sought public comment on issues involving preemption. Additionally, after issuing its proposal, the Department specifically invited a number of groups representing the interests of States and their legislators to meet with the

Department to discuss the proposed regulations. These groups were: the National League of Cities, the National Association of Counties, the National Conference of State Legislators, the County Executives of America, the International City/County Management Association, the American Legislative Exchange Council, the National Emergency Management Association/CSG Council of State Governments, the International Association of Emergency Managers, the National Governors Association, and the United States Conference of Mayors.

The Department received numerous comments in response to its invitations. States, the private sector, academia, various interest groups, and individual members of Congress submitted comments. The commenters were divided in their views of the proposed approach on preemption. A number of commenters favored the Department's proposal, while others opposed it. Some commenters misunderstood the Department's position on preemption or the current state of the case law on preemption. As discussed below, the Department is clarifying its approach on preemption in certain respects. Specifically, we confirm: the propriety of discussing the Department's view on preemption, though Congress was silent on the question; that the type of preemption called for by Section 550 is not field preemption, but conflict preemption; and that the Department will further assist in the process of determining whether a non-Federal regulation is preempted by providing opinions regarding the impact of that regulation on the Federal scheme.

2. Propriety of Department's views on preemption

As an initial matter, some commenters, including Members of Congress, suggested that, since Congress was silent on preemption, the Department's rulemaking

should be silent as well. The comments on this subject touch on two important subtopics: who (i.e., which government structure) should determine the preemptive effect of Section 550 and the regulatory program promulgated under its authority; and what law, if any, the regulatory program under Section 550 might preempt.

In Section 550, Congress did not expressly speak to the issue of preemption. Preemption questions following statutory silence on preemption are not novel. Courts and agencies have previously faced and dealt with who decides preemption issues in the face of congressional silence. It is helpful to recall that, as a general matter, Congress often provides the Executive Branch with authority to administer a regulatory program while leaving gaps or ambiguities in the authorizing law. When this happens, the Supreme Court has long recognized that agencies have the responsibility, within the general delegation, to formulate policy and make rules to fill those gaps and interpret the ambiguities. See Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837, 843 (1984) ("The power of an administrative agency to administer a congressionally created . . . program necessarily requires the formulation of policy and the making of rules to fill any gap left, implicitly or explicitly by Congress.") (ellipses in original; citation omitted). Agencies, not only the courts, exercise their expertise to fill in the gaps and interpret the ambiguities. See id. at 843 & n.11 ("If, however, the court determines that Congress has not directly addressed the precise question at issue, the court does not simply impose its own construction on the statute . . . Rather, if the statute is silent or ambiguous with respect to the specific issue, the question for the court is whether the agency's answer is based on a permissible construction of the statute. The court need not conclude that the agency construction was the only one it permissibly

could have adopted to uphold the construction, or even the reading the court would have reached if the question initially had arisen in a judicial proceeding."). And even if a court interprets an ambiguous statute before an agency promulgates rules to fill the gaps or interpret the ambiguities, the court's interpretation does not necessarily restrict the agency's ability to adopt a different interpretation in the future. See National Cable & Telecomm. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 982 (2005).

This does not mean to slight the courts' role in the interpretive process. As the Supreme Court has stated, "The judiciary is the final authority on issues of statutory construction and must reject administrative constructions which are contrary to clear congressional intent." Chevron, 467 U.S. at 843 n.9.

With respect to the issue of preemption in particular, the Supreme Court has applied these same principles regarding Congress, the courts and the agencies. See, e.g., Fidelity Fed. Sav. and Loan Ass'n v. de la Cuesta, 458 U.S. 141, 151-54 (1982). "Federal regulations have no less pre-emptive effect than federal statutes. . . . A pre-emptive regulation's force does not depend on express congressional authorization to displace state law." Id. at 153-54. The Supreme Court, and lower courts, have given deference to agencies that define, through regulation, the scope of preemption. See, e.g., id.; Wachovia Bank, N.A. v. Burke, 414 F.3d 305 (2d Cir. 2005).

So although some commenters claimed that the Department lacks the authority to address the issue of preemption in its regulations or later-issued opinions, this assertion is simply not consistent with current law. Federal agencies have historically published their views on the preemptive effect of federal law in a number of contexts. See, e.g., In re Wireless Consumers Alliance, Inc., 15 F.C.C.R. 17,021 (Aug. 14, 2000) (administrative

agency opinion on preemptive effect of federal law); 1999 WL 303948 (April 20, 1999) (U.S. Department of Labor Release discussing views on preemption of state laws). We anticipate that the courts will ultimately resolve any preemption question, with an appropriate level of deference to the position of the agency.

Some comments urged the Department to avoid preemption after looking to a canon of interpretation involving a presumption against preemption. This presumption, however, typically exists "in areas of regulation that are traditionally allocated to states and are of particular local concern." Wachovia Bank, N.A., 414 F.3d at 314; see also United States v. Locke, 529 U.S. 89 (2000). As noted in the Advance Notice, measures to prevent terrorist attacks against the Nation's critical infrastructure do not involve an area traditionally regulated by the States. Very few state and local jurisdictions currently regulate security at chemical facilities.

The Department recognizes that courts sometimes look to legislative intent with respect to the issue of preemption – decisions in this area are replete with such references. See, e.g., Medtronic, Inc. v. Lohr, 518 U.S. 470, 485 (1996). In the context of Section 550, however, it is very difficult to discern that intent. The legislative history on the point is mixed, with various Members of Congress making floor statements that are not consistent with each other. See, e.g., Cong. Rec. H7967 (daily ed. Sept. 29, 2006) (statement of Rep. King) ("the intention is not to preempt the ability of the States") and Cong. Rec. S10619 (daily ed. Sept. 29, 2006) (statement of Sen. Voinovich) ("I feel strongly that this provision sets that uniform set of rules and in so doing, impliedly preempts further regulation by State rules or laws.") In addition, it is particularly difficult to gauge congressional intent on one relatively short, page-and-a half authorizing

provision in a lengthy appropriations act that runs over 100 pages. To be sure, individual members of Congress – including some members substantially involved in homeland security issues – have expressed strong views on preemption. But can it really be said that legislative intent may be discerned on the silent aspect of one authorizing section of a lengthy appropriations act? Cf. Chrysler Corp. v. Brown, 441 U.S. 281, 311-12 (1979); Castaneda-Gonzalez v. INS, 564 F.2d 417, 424 (D.C. Cir. 1977).

As an additional consideration, the Department notes that if it were to disclaim any preemptive effect of the regulatory program under Section 550, it would create an inconsistency with the Department's own regime for regulating chemical facilities under the MTSA. In its regulations under MTSA, the Department has stated its view that the principles of conflict preemption apply. See 68 Fed. Reg. 60,468 (Oct. 22, 2003). Congress has charged the Department with implementing the security programs under both MTSA and Section 550, and the Department seeks to implement these programs in a consistent and logical manner.

3. No field preemption

Some commenters feared—and others hoped—that the Department's approach to preemption would wholly displace state and local laws. This is incorrect. The Department does not in this interim final rule claim that the "field preemption" doctrine applies in this regulatory context. The Department does not view its regulatory scheme as one which so fully occupies the field as to pre-empt any state law touching the same subject.

This is clear from the statutory text. For example, the authority granted in Section 550 calls for the federal regulations to apply to facilities that present "high levels of

security risk" as determined by the Secretary. The Department does not, therefore, have authority under Section 550 to regulate facilities that may, in the Secretary's view, present other than high levels of security risk. Some facilities may not be deemed by the Department as presenting a high risk. These facilities may be regulated by States provided such regulation is not otherwise in conflict with the federal program. In addition, as mentioned in the comments, Section 550 specifically allows the Secretary to approve alternative security programs that may have been submitted in response to State or local authorities.

4. Principles of conflict preemption

Even for high risk facilities, the approach outlined in the Advance Notice, and further developed here, is one of conflict preemption. Conflict preemption is established in the Constitution and has been developed in case law (see, e.g., Geier v. American Honda Motor Co., 529 U.S. 861, 873 (2000); Fidelity Fed. Sav. and Loan Ass'n v. de la Cuesta, 458 U.S. 141, 152 (1982); Surrick v. Killion, 449 F.3d 520, 530-31 (3d Cir. 2006)), and the well-known standards of conflict preemption—which are captured in the regulatory text at § 27.405—apply to Section 550 and this regulation.

After considering comments, however, the Department has modified certain of its prior statements on preemption as potentially too broad. In the Advance Notice, the Department noted that Section 550 compels the Department to preserve chemical facilities' flexibility to choose security measures to reach the appropriate security outcome. The Department went on to say that a State measure frustrating this balance "will be preempted." The Department has decided, however, that clarification is in order, as this regulation is not intended to be the equivalent of "field preemption" for facilities

determined to be high risk. Instead, it is only meant to indicate that the regulation is not to be conflicted by, interfered with, hindered by or frustrated by State measures, under long-standing legal principles.

Only a few jurisdictions have developed security regulations (rather than health, safety, and environmental regulations) governing chemical sites. While we have not canvassed all existing state laws and regulations, currently we have no reason to conclude that any such non-Federal measure is being applied in a way that would impede the performance standards or other provisions of Section 550 and this Interim Final Rule. However, concrete conclusions about the effect of state laws and the application of preemption principles will require an understanding of future, factual contexts in which those laws are applied. The Department will consider any problems that arise in this regard in a more particularized manner.

Consistent with the approach outlined in the Advance Notice, the Department will entertain requests for its views on particular state or local laws, which will be issued by way of an opinion. In addition to the approach described in the Advanced Notice, the Department will seek the input and views of a State before finalizing the Department's view of preemption with respect to such State's laws. See § 27.405(d)(3). It will be helpful for the Department to seek the views of the relevant States if an opinion on preemption is requested under these regulations. Additionally, the Department would, time permitting, seek public notice and comment before formulating its views on a particular preemption question, consistent, of course, with the congressional mandate to protect from public disclosure information submitted under Section 550. The Department,

however, declines to add additional procedural formalities to the regulation as it relates to preemption.

Certain commenters asked that the Advance Notice be more clear in delineating what state laws are not to be preempted. The Department does not intend to preempt existing health, safety and environmental regulations. In the future, however, if state or local governments enact security laws or promulgate security regulations under the rubric of health, safety, or environmental protections, those laws and regulations will be measured against the standard described in § 27.405. Of course, non-Federal regulations that fall below federal performance standards will not diminish the federal requirements that covered facilities must meet.

D. Unfunded Mandates Reform Act

Title II of the Unfunded Mandates Reform Act of 1995 (UMRA), enacted as Pub. L. No. 104-4 on March 22, 1995, requires each Federal agency, to the extent permitted by law, to prepare a written assessment of the effects of any Federal mandate in a proposed or final agency rule that may result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more (adjusted annually for inflation) in any one year. Section 204(a) of UMRA, 2 U.S.C. 1534(a), requires the Federal agency to develop an effective process to permit timely input by elected officers (or their designees) of State, local, and tribal governments on a proposed "significant intergovernmental mandate." A "significant intergovernmental mandate" under the UMRA is any provision in a Federal agency regulation that will impose an enforceable duty upon State, local, and tribal governments, in the aggregate, of $100 million (adjusted annually for inflation) in any one year. Section 203 of UMRA, 2

U.S.C. 1533, which supplements section 204(a), provides that before establishing any regulatory requirements that might significantly or uniquely affect small governments, the agency shall have developed a plan that, among other things, provides for notice to potentially affected small governments, if any, and for a meaningful and timely opportunity to provide input in the development of regulatory proposals. The Department sought input from state and local governments during the comment period and hosted a meeting with state and local representatives on February 6, 2007. A list of participants and short description of the meeting is in the docket.

This interim final rule would result in expenditure by the private sector of $100 million (adjusted annually for inflation) or more in any one year. At this time, however, we do not have enough information regarding the specific facilities that will be required to comply with the rule's risk-based performance standards in order to know if this interim final rule will impose an enforceable duty upon State, local, and tribal governments of $100 million (adjusted annually for inflation) or more in any one year. DHS has conducted a "Regulatory Assessment," which explains the economic effects of the rule. The "Regulatory Assessment" is summarized in the section entitled "Executive Order 12866," and a copy may be found in the public docket for this IFR.

As explained in the "Regulatory Assessment," DHS's preliminary estimate of the total number of high-risk chemical facilities that will be covered by the risk-based performance measures required by this rule ranges from 1,500 to 6,500 chemical facilities. This estimate is based on currently available information. After chemical facilities fitting certain risk profiles complete the Top-Screen risk assessment methodology (which will be accessible through a secure Department website), DHS will

better understand how many and which specific chemical facilities will be deemed to be "high-risk" for the purposes of this rule. For the purposes of this discussion, we believe this rule may require certain municipalities that own and/or operate power generating facilities to purchase security enhancements, but at this time we do not know the extent of the financial impact.

E. Paperwork Reduction Act

This interim final rule contains collection of information requirements under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501–3520). "Collection of information," as defined in 5 CFR § 1320.3(c), includes reporting, record keeping, monitoring, posting, labeling, and other similar actions.

Under Section 550 of the DHS Appropriations Act, the Department will use the Chemical Security Assessment Tool (CSAT) system to collect and analyze key data from chemical facilities to: (1) Identify facilities that present a high level of risk, (2) Support the facility-specific judgment for preliminary and final tier high risk determinations, (3) Specify the facility-specific security concerns that facilities must address in their SVAs and SSPs, and (4) Collect the facility-specific security measures, activities, and systems for judging compliance against the risk based performance standards. DHS will submit the collections for SVAs and the SSPs during the summer months.

This rule introduces a new collection, 1670-NEW, with two new forms: User Registration (DHS 9002 (1/07)) and Top Screen (DHS 9007 (2/07)). As such, DHS has submitted the following information requirements to OMB for its review:

TITLE: Chemical Security Assessment Tool (CSAT): User Registration

OMB Control Number: 1670_NEW

Summary of Collection of Information: Section 550 provided the Department with the authority to regulate high risk chemical facilities. Further, it requires that the Secretary of the Department of Homeland Security identify high risk facilities and provide for the protection of the information regarding and provided by those facilities. DHS has identified the CSAT system as the Information Technology (IT) system it will use to obtain and quantify this key risk data from facilities. The Department will begin collecting information upon the effective date of this interim final rule.

Use Of: The Department will use the registration information as a basis for providing chemical facilities access to the CSAT system.

Need for Information The Department needs the information from the User Registration form to identify and vet requests to access the CSAT system.

Description of the Respondents: DHS anticipates that there will 40,000 respondents in the first year. The respondents will be the owners and operators of the chemical facilities that will need to submit information through the CSAT system.

Frequency of Response: On Occasion.

Annual Burden Estimate: Each facility is estimated to have a burden of 44.5 minutes to complete DHS Form 9002 (1/07). The annual hour burden is estimated to be 22,250.

TITLE: Chemical Security Assessment Tool (CSAT): Top Screen

Summary of Collection of Information: Section 550 provided the Department with the authority to regulate high risk chemical facilities. Further, it requires that the Secretary of the Department of Homeland Security identify high risk facilities and provide for the

protection of the information regarding and provided by those facilities. DHS has identified the CSAT system as the Information Technology (IT) system it will use to obtain and quantify this key risk data from facilities. The Department will begin collecting information upon the effective date of this interim final rule.

Use of: The CSAT is the Department's system for collecting and analyzing key data from chemical facilities to: (1) Identify facilities that present a high level of risk, (2) Support the facility-specific judgment for preliminary and final tier determinations, and (3) Specify the facility-specific security concerns that facilities must address in their SVAs and SSPs.

Respondents (including number of): DHS anticipates there will 40,000 respondents in the first year. The respondents will be chemical facilities that possess, or plan to possess, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criteria identified by the Department.

Frequency: Most facilities will complete the Top-Screen once. The Department will require facilities that are determined to be high risk to periodically resubmit the Top-Screen.

Burden of Response: Depending upon the size of the facility, the burden rates will vary. The estimated burden hours for the different facility types are detailed in the table below. The combined hour burden for all facilities completing the Top-Screen is estimated to be 1,230,550. The combined annual cost burden for the User Registration and the Top-Screen is $110,003,900.

Table 2. Summary of Burden Hours for Conducting User Registration (DHS Form 9002 (1/07)) and Top Screen (DHS Form 9007 (2/07))

Type of Facility	Number of Facilities	Hour Burden per Facility	Total hour Burden

Open Large	9,327	39.5	**368,400**
Merchant Wholesalers	432	30	**13,000**
Facilities with only 1- 2 chemicals	7,968	25.5	**203,200**
Other	22,273	30	**668,200**
TOTAL			**1,252,800**

As required by the Paperwork Reduction Act of 1995 (44 U.S.C. 3507 (d)), we have submitted a copy of the interim final rule to OMB for its review of the collections of information. Due to the circumstances surrounding this final rule, we ask for emergency processing.

DHS is soliciting comments to:

(1) Evaluate whether the proposed information requirement is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including using appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Individuals and organizations may submit comments on the information collection requirements by [Date 90 days after publication in the **Federal Register**]. Direct the comments to the address listed in the **ADDRESSES** section of this document.

Also, fax a copy of the comments to the Office of Information and Regulatory Affairs, Office of Management and Budget at 202-395-6974, Attention: Nathan Lesser, DHS Desk Officer; and send via electronic mail to oira_submission@omb.eop.gov.

A comment to OMB is most effective if OMB receives it within 30 days of publication. DHS will publish the OMB control number for this information collection in the **Federal Register** after OMB approves it.

Under the protections provided by the PRA, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

F. National Environmental Policy Act

In the Advance Notice, the Department reviewed the rulemaking process with regard to the National Environmental Policy Act (NEPA). See 71 FR 78276, 78294 (Dec. 28, 2006). Specifically, the Department considered the short timeframe to issue these interim final regulations and the statutory mandate, which directed that each chemical facility develop and implement site security plans, with the proviso that the facility could select layered security measures to appropriately address the vulnerability assessment and the risk-based performance standards for security of the facility. Additionally, Congress mandated that the Secretary could not disapprove a site security plan based on the presence or absence of a particular security measure, but only on the failure to satisfy a risk-based performance standard.

Chemical facilities are of a wide variety of designs and sizes, and are located in a wide range of geographic settings, communities, and natural environments. The Department is not funding or directing specific measures under these regulations, but

issuing performance standards. Consequently, the Department currently has no way to determine the action the chemical facility will take to meet the standards, and what effect any action might have on the environment. Even if the Department could predict the actions the facilities would take in response to the standards, it is likely facilities would take widely varying actions to comply, based upon type of facility, geographic location, existing infrastructure, etc.

We received no comments objecting to this conclusion during the comment period, and further, no comments on this matter were raised during the Environmental Organizations Forum the Department hosted on January 17, 2007. Accordingly, the information needed to conduct an Environmental Impact Statement is not available at this time and, in any event, the Department could not reasonably conduct an Environmental Impact Statement within the six months time allotted for issuance of the interim final regulations.

List of Subjects

Chemical security, Facilities, Incorporation by Reference, Reporting and recordkeeping, Security measures.

The Interim Final Rule

For the reasons set forth in the preamble, the Department of Homeland Security adds Part 27 to Title 6, Code of Federal Regulations, to read as follows:

Title 6--Department of Homeland Security

Chapter 1--Department of Homeland Security, Office of the Secretary

PART 27--CHEMICAL FACILITY ANTI-TERRORISM STANDARDS

1. The authority citation for Part 27 reads as follows:

Authority: Pub. L. 109-295, sec. 550.

2. Add Part 27 to read as follows:

Subpart A--General

Subpart B--Chemical Facility Security Program

Subpart C—Orders and Adjudications

Authority: Pub. L. 109-295, sec. 550.

Subpart A--General

§ 27.100 Purpose.

The purpose of this Part is to enhance the security of our Nation by furthering the mission of the Department as provided in 6 U.S.C. § 111(b)(1) and by lowering the risk posed by certain chemical facilities.

§ 27.105 Definitions.

Alternative Security Program or ASP shall mean a third-party or industry organization program, a local authority, state or Federal government program or any element or aspect thereof, that the Assistant Secretary has determined meets the requirements of this Part and provides for an equivalent level of security to that established by this Part.

Assistant Secretary shall mean the Assistant Secretary for Infrastructure Protection, Department of Homeland Security or his designee.

Chemical Facility or facility shall mean any establishment that possesses or plans to possess, at any relevant point in time, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criteria identified by the Department. As used herein, the term chemical facility or facility shall also refer to the owner or operator of the chemical facility. Where multiple owners and/or operators function within a common infrastructure or within a single fenced area, the Assistant Secretary may determine that such owners and/or operators constitute a single chemical facility or multiple chemical facilities depending on the circumstances.

Chemical Security Assessment Tool or CSAT shall mean a suite of four applications, including User Registration, Top-Screen, Security Vulnerability Assessment, and Site Security Plan, through which the Department will collect and analyze key data from chemical facilities.

Chemical-terrorism Vulnerability Information or CVI shall mean the information listed in § 27.400(b).

Coordinating Official shall mean the person (or his designee(s)) selected by the Assistant Secretary to ensure that the regulations are implemented in a uniform, impartial, and fair manner.

Covered Facility or Covered Chemical Facility shall mean a chemical facility determined by the Assistant Secretary to present high levels of security risk, or a facility that the Assistant Secretary has determined is presumptively high risk under § 27.200.

Department shall mean the Department of Homeland Security.

Deputy Secretary shall mean the Deputy Secretary of the Department of Homeland Security or his designee.

Director of the Chemical Security Division or Director shall mean the Director of the Chemical Security Division, Office of Infrastructure Protection, Department of Homeland Security or any successors to that position within the Department or his designee.

General Counsel shall mean the General Counsel of the Department of Homeland Security or his designee.

Operator shall mean a person who has responsibility for the daily operations of a facility or facilities subject to this Part.

Owner shall mean the person or entity that owns any facility subject to this Part.

Present high levels of security risk and high risk shall refer to a chemical facility that, in the discretion of the Secretary of Homeland Security, presents a high risk of significant adverse consequences for human life or health, national security and/or critical economic assets if subjected to terrorist attack, compromise, infiltration, or exploitation.

Risk profiles shall mean criteria identified by the Assistant Secretary for

determining which chemical facilities will complete the Top-Screen or provide other risk assessment information.

Screening Threshold Quantity or STQ shall mean the quantity of a chemical of interest, upon which the facility's obligation to complete and submit the CSAT Top-Screen is based.

Secretary or Secretary of Homeland Security shall mean the Secretary of the Department of Homeland Security or any person, officer or entity within the Department to whom the Secretary's authority under Section 550 is delegated.

Terrorist attack or terrorist incident shall mean any incident or attempt that constitutes terrorism or terrorist activity under 6 U.S.C. 101(15) or 18 U.S.C. 2331(5) or 8 U.S.C. 1182(a)(3)(B)(iii), including any incident or attempt that involves or would involve sabotage of chemical facilities or theft, misappropriation or misuse of a dangerous quantity of chemicals.

Tier shall mean the risk level associated with a covered chemical facility and which is assigned to a facility by the Department. For purposes of this part, there are four risk-based tiers, ranging from highest risk at Tier 1 to lowest risk at Tier 4.

Top-Screen shall mean an initial screening process designed by the Assistant Secretary through which chemical facilities provide information to the Department for use pursuant to § 27.200 of these regulations.

Under Secretary shall mean the Under Secretary for National Protection and Programs, Department of Homeland Security or any successors to that position within the Department or his designee.

§ 27.110 Applicability.

(a) This Part applies to chemical facilities and to covered facilities as set out herein.

(b) This Part does not apply to facilities regulated pursuant to the Maritime Transportation Security Act of 2002, Pub. L. 107-295, as amended; Public Water Systems, as defined by Section 1401 of the Safe Drinking Water Act, Pub. L. 93-523, as amended; Treatment Works as defined in Section 212 of the Federal Water Pollution Control Act, Pub. L. 92-500, as amended; any facility owned or operated by the Department of Defense or the Department of Energy, or any facility subject to regulation by the Nuclear Regulatory Commission.

§ 27.115 Implementation.

The Assistant Secretary may implement the Section 550 program in a phased manner, selecting certain chemical facilities for expedited initial processes under these regulations and identifying other chemical facilities or types or classes of chemical facilities for other phases of program implementation. The Assistant Secretary has flexibility to designate particular chemical facilities for specific phases of program implementation based on potential risk or any other factor consistent with this Part.

§ 27.120 Designation of a coordinating official; Consultations and technical assistance.

(a) The Assistant Secretary will designate a Coordinating Official who will be responsible for ensuring that these regulations are implemented in a uniform, impartial, and fair manner.

(b) The Coordinating Official and his staff shall provide guidance to covered facilities regarding compliance with this Part and shall, as necessary and to the extent that resources permit, be available to consult and to provide technical assistance to an owner or operator who seeks such consultation or assistance.

(c) In order to initiate consultations or seek technical assistance, a covered facility shall submit a written request for consultation or technical assistance to the Coordinating Official or contact the Department in any other manner specified in any subsequent guidance. Requests for consultation or technical guidance do not serve to toll any of the applicable timelines set forth in this Part.

(d) If a covered facility modifies its facility, processes, or the types or quantities of materials that it possesses, and believes that such changes may impact the covered facility's obligations under this Part, the covered facility may request a consultation with the Coordinating Official as specified in paragraph (c).

§ 27.125 Severability.

If a court finds any portion of this Part to have been promulgated without proper authority, the remainder of this Part will remain in full effect.

Subpart B--Chemical Facility Security Program

§ 27.200 Information regarding security risk for a chemical facility.

(a) Information to determine security risk. In order to determine the security risk posed by chemical facilities, the Secretary may, at any time, request information from chemical facilities that may reflect potential consequences of or vulnerabilities to a terrorist attack or incident, including questions specifically related to the nature of the business and activities conducted at the facility; information concerning the names, nature, conditions of storage, quantities, volumes, properties, customers, major uses, and other pertinent information about specific chemicals or chemicals meeting a specific criterion; information concerning facilities' security, safety, and emergency response practices, operations, and procedures; information regarding incidents, history, funding, and other matters bearing on the effectiveness of the security, safety and emergency response programs, and other information as necessary.

(b) Obtaining information from facilities.

(1) The Assistant Secretary may seek the information provided in paragraph (a) by contacting chemical facilities individually or by publishing a notice in the **Federal Register** seeking information from chemical facilities that meet certain criteria, which the Department will use to determine risk profiles. Through any such individual or **Federal Register** notification, the Assistant Secretary may instruct such facilities to complete and submit a Top-Screen process, which may be completed through a secure Department Web site or through other means approved by the Assistant Secretary.

(2) A facility must complete and submit a Top-Screen in accordance with the schedule provided in § 27.210 if it possesses any of the chemicals listed in Appendix A at the corresponding Screening Threshold Quantities.

(3) Where the Department requests that a facility complete and submit a Top-Screen, the facility must designate a person who is responsible for the submission of information through the CSAT system and who attests to the accuracy of the information contained in any CSAT submissions. Such submitter must be an officer of the corporation or other person designated by an officer of the corporation and must be domiciled in the United States.

(c) Presumptively High Risk Facilities.

(1) If a chemical facility subject to paragraph (a) or (b) of this section fails to provide information requested or complete the Top-Screen within the timeframe provided in § 27.210, the Assistant Secretary may, after attempting to consult with the facility, reach a preliminary determination, based on the information then available, that the facility presumptively presents a high level of security risk. The Assistant Secretary shall then issue a notice to the entity of this determination and, if necessary, order the facility to provide information or complete the Top-Screen pursuant to these rules. If the facility then fails to do so, it may be subject to civil penalties pursuant to § 27.300, audit and inspection under § 27.250 or, if appropriate, an order to cease operations under § 27.300.

(2) If the facility deemed "presumptively high risk" pursuant to subsection (c)(1) completes the Top-Screen, and the Department determines that it does not present a high level of security risk under § 27.205, its status as "presumptively high risk" will terminate, and the Department will issue a notice to the facility to that effect.

§ 27.205 Determination that a chemical facility "presents a high level of security risk."

(a) Initial Determination. The Assistant Secretary may determine at any time that a chemical facility presents a high level of security risk based on any information available (including any information submitted to the Department under § 27.200) that, in the Secretary's discretion, indicates the potential that a terrorist attack involving the facility could result in significant adverse consequences for human life or health, national security or critical economic assets. Upon determining that a facility presents a high level of security risk, the Department shall notify the facility in writing of such initial determination and may also notify the facility of the Department's preliminary determination of the facility's placement in a risk-based tier pursuant to § 27.220(a).

(b) Redetermination. If a covered facility previously determined to present a high level of security risk has materially altered its operations, it may seek a redetermination by filing a Request for Redetermination with the Assistant Secretary, and may request a meeting regarding the Request. Within 45 calendar days of receipt of such a Request, or within 45 calendar days of a meeting under this paragraph, the Assistant Secretary shall notify the covered facility in writing of the Department's decision on the Request for Redetermination.

§ 27.210 Submissions schedule.

(a) Initial Submission. The timeframes in paragraphs (a)(2) and (a)(3) also apply to covered facilities that submit an Alternative Security Program pursuant to § 27.235.

(1) Top-Screen. Facilities shall complete and submit a Top-Screen within the following time frames:

(i) This paragraph is operative on the date that the Department publishes a final Appendix A. Unless otherwise notified, within 60 calendar days of the effective date of Appendix A for facilities that possess any of the chemicals listed in Appendix A at the corresponding STQs, or within 60 calendar days for facilities that come into possession of any of the chemicals listed in Appendix A at the corresponding STQs; or

(ii) Within the time frame provided in any written notification from the Department or specified in any subsequent **Federal Register** notice.

(2) Security Vulnerability Assessment. Unless otherwise notified, a covered facility must complete and submit a Security Vulnerability Assessment within 90 calendar days of written notification from the Department or within the time frame specified in any subsequent **Federal Register** notice.

(3) Site Security Plan. Unless otherwise notified, a covered facility must complete and submit a Site Security Plan within 120 calendar days of written notification from the Department or within the time frame specified in any subsequent **Federal Register** notice.

(b) Resubmission Schedule for Covered Facilities. The timeframes in this subsection also apply to covered facilities who submit an Alternative Security Program pursuant to § 27.235.

(1) Top-Screen. Unless otherwise notified, Tier 1 and Tier 2 covered facilities must complete and submit a new Top-Screen no less than two years, and no more than two years and 60 calendar days, from the date of the Department’s approval of the facility's Site Security Plan; and Tier 3 and Tier 4 covered facilities must complete and

submit a Top-Screen no less than 3 years, and no more than 3 years and 60 calendar days, from the date of the Department's approval of the facility's Site Security Plan.

(2) Security Vulnerability Assessment. Unless otherwise notified and following a Top-Screen resubmission pursuant to paragraph (b)(1), a covered facility must complete and submit a new Security Vulnerability Assessment within 90 calendar days of written notification from the Department or within the time frame specified in any subsequent **Federal Register** notice.

(3) Site Security Plan. Unless otherwise notified and following a Security Vulnerability Assessment resubmission pursuant to paragraph (b)(2), a covered facility must complete and submit a new Site Security Plan within 120 calendar days of written notification from the Department or within the time frame specified in any subsequent **Federal Register** notice.

(c) The Assistant Secretary retains the authority to modify the schedule in this Part as needed. The Assistant Secretary may shorten or extend these time periods based on the operations at the facility, the nature of the covered facility's vulnerabilities, the level and immediacy of security risk, or for other reasons. If the Department alters the time periods for a specific facility, the Department will do so in written notice to the facility.

(d) If a covered facility makes material modifications to its operations or site, the covered facility must complete and submit a revised Top-Screen to the Department within 60 days of the material modification. In accordance with the resubmission requirements in § 27.210(b)(2) and (3), the Department will notify the covered facility as

to whether the covered facility must submit a revised Security Vulnerability Assessment, Site Security Plan, or both.

§ 27.215 Security vulnerability assessments.

(a) Initial Assessment. If the Assistant Secretary determines that a chemical facility is high-risk, the facility must complete a Security Vulnerability Assessment. A Security Vulnerability Assessment shall include:

(1) Asset Characterization, which includes the identification and characterization of potential critical assets; identification of hazards and consequences of concern for the facility, its surroundings, its identified critical asset(s), and its supporting infrastructure; and identification of existing layers of protection;

(2) Threat Assessment, which includes a description of possible internal threats, external threats, and internally-assisted threats;

(3) Security Vulnerability Analysis, which includes the identification of potential security vulnerabilities and the identification of existing countermeasures and their level of effectiveness in both reducing identified vulnerabilities and in meeting the applicable Risk-Based Performance Standards;

(4) Risk Assessment, including a determination of the relative degree of risk to the facility in terms of the expected effect on each critical asset and the likelihood of a success of an attack; and

(5) Countermeasures Analysis, including strategies that reduce the probability of a successful attack or reduce the probable degree of success, strategies that enhance

the degree of risk reduction, the reliability and maintainability of the options, the capabilities and effectiveness of mitigation options, and the feasibility of the options.

(b) Except as provided in § 27.235, a covered facility must complete the Security Vulnerability Assessment through the CSAT process, or through any other methodology or process identified or issued by the Assistant Secretary.

(c) Covered facilities must submit a Security Vulnerability Assessment to the Department in accordance with the schedule provided in § 27.210.

(d) Updates and Revisions.

(1) A covered facility must update and revise its Security Vulnerability Assessment in accordance with the scheduled provided in § 27.210.

(2) Notwithstanding paragraph (d)(1), a covered facility must update, revise or otherwise alter its Security Vulnerability Assessment to account for new or differing modes of potential terrorist attack or for other security-related reasons, if requested by the Assistant Secretary.

§ 27.220 Tiering.

(a) Preliminary Determination of Risk-Based Tiering. Based on the information the Department receives in accordance with §§ 27.200 and 27.205 (including information submitted through the Top-Screen process) and following its initial determination in § 27.205(a) that a facility presents a high level of security risk, the Department shall notify a facility of the Department's preliminary determination of the facility's placement in a risk-based tier.

(b) Confirmation or Alteration of Risk-Based Tiering: Following review of a covered facility's Security Vulnerability Assessment, the Assistant Secretary shall notify the covered facility of its final placement within a risk-based tier, or for covered facilities previously notified of a preliminary tiering, confirm or alter such tiering.

(c) The Department shall place covered facilities in one of four-risk based tiers, ranging from highest risk facilities in Tier 1 to lowest risk facilities in Tier 4.

(d) The Assistant Secretary may provide the facility with guidance regarding the risk-based performance standards and any other necessary guidance materials applicable to its assigned tier.

§ 27.225 Site security plans.

(a) The Site Security Plan must meet the following standards:

(1) Address each vulnerability identified in the facility’s Security Vulnerability Assessment, and identify and describe the security measures to address each such vulnerability;

(2) Identify and describe how security measures selected by the facility will address the applicable risk-based performance standards and potential modes of terrorist attack including, as applicable, vehicle-borne explosive devices, water borne explosive devices, ground assault, or other modes of potential modes identified by the Department;

(3) Identify and describe how security measures selected and utilized by the facility will meet or exceed each applicable performance standard for the appropriate risk-based tier for the facility; and

(4) Specify other information the Assistant Secretary deems necessary regarding chemical facility security.

(b) Except as provided in § 27.235, a covered facility must complete the Site Security Plan through the CSAT process, or through any other methodology or process identified or issued by the Assistant Secretary.

(c) Covered facilities must submit a Site Security Plan to the Department in accordance with the schedule provided in § 27.210.

(d) Updates and Revisions.

(1) When a covered facility updates, revises or otherwise alters its Security Vulnerability Assessment pursuant to § 27.215(d), the covered facility shall make corresponding changes to its Site Security Plan.

(2) A covered facility must also update and revise its Site Security Plan in accordance with the schedule in § 27.210.

(e) A covered facility must conduct an annual audit of its compliance with its Site Security Plan.

§ 27.230 Risk-based performance standards.

(a) Covered facilities must satisfy the performance standards identified in this section. The Assistant Secretary will issue guidance on the application of these standards to risk-based tiers of covered facilities, and the acceptable layering of measures used to meet these standards will vary by risk-based tier. Each covered facility must select, develop in their Site Security Plan, and implement appropriately risk-based measures designed to satisfy the following performance standards:

(1) Restrict Area Perimeter. Secure and monitor the perimeter of the facility;

(2) Secure Site Assets. Secure and monitor restricted areas or potentially critical targets within the facility;

(3) Screen and Control Access. Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including,

(i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and

(ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures;

(4) Deter, Detect, and Delay. Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to:

(i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;

(ii) Deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets;

(iii) Detect attacks at early stages, through countersurveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and

(iv) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning;

(5) Shipping, Receipt, and Storage. Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility;

(6) Theft and Diversion. Deter theft or diversion of potentially dangerous chemicals;

(7) Sabotage. Deter insider sabotage;

(8) Cyber. Deter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS); critical business systems; and other sensitive computerized systems;

(9) Response. Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders;

(10) Monitoring. Maintain effective monitoring, communications and warning systems, including,

(i) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained;

(ii) Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department; and

(iii) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions;

(11) Training. Ensure proper security training, exercises, and drills of facility personnel;

(12) Personnel Surety. Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including,

(i) measures designed to verify and validate identity;

(ii) measures designed to check criminal history;

(iii) measures designed to verify and validate legal authorization to work; and

(iv) measures designed to identify people with terrorist ties;

(13) Elevated Threats. Escalate the level of protective measures for periods of elevated threat;

(14) Specific Threats, Vulnerabilities, or Risks. Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;

(15) Reporting of Significant Security Incidents. Report significant security incidents to the Department and to local law enforcement officials;

(16) Significant Security Incidents and Suspicious Activities. Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;

(17) Officials and Organization. Establish official(s) and an organization responsible for security and for compliance with these standards;

(18) Records. Maintain appropriate records; and

(19) Address any additional performance standards the Assistant Secretary may specify.

§ 27.235 Alternative security program.

(a) Covered facilities may submit an Alternate Security Program (ASP) pursuant to the requirements of this section. The Assistant Secretary may approve an Alternate Security Program, in whole, in part, or subject to revisions or supplements, upon a determination that the Alternate Security Program meets the requirements of this Part and provides for an equivalent level of security to that established by this Part.

(1) A Tier 4 facility may submit an ASP in lieu of a Security Vulnerability Assessment, Site Security Plan, or both.

(2) Tier 1, Tier 2, or Tier 3 facilities may submit an ASP in lieu of a Site Security Plan. Tier 1, Tier 2, and Tier 3 facilities may not submit an ASP in lieu of a Security Vulnerability Assessment.

(b) The Department will provide notice to a covered facility about the approval or disapproval, in whole or in part, of an ASP, using the procedure specified in § 27.240 if the ASP is intended to take the place of a Security Vulnerability Assessments, or using

the procedure specified in § 27.245 if the ASP is intended to take the place of a Site Security Plan.

§ 27.240 Review and approval of security vulnerability assessments.

(a) Review and Approval. The Department will review and approve in writing all Security Vulnerability Assessments that satisfy the requirements of § 27.215, including Alternative Security Programs submitted pursuant to § 27.235.

(b) If a Security Vulnerability Assessment does not satisfy the requirements of § 27.215, the Department will provide the facility with a written notification that includes a clear explanation of deficiencies in the Security Vulnerability Assessment. The facility shall then enter further consultations with the Department and resubmit a sufficient Security Vulnerability Assessment by the time specified in the written notification provided by the Department under this section. If the resubmitted Security Vulnerability Assessment does not satisfy the requirements of § 27.215, the Department will provide the facility with written notification (including a clear explanation of deficiencies in the SVA) of the Department's disapproval of the SVA.

§ 27.245 Review and approval of site security plans.

(a) Review and Approval.

(1) The Department will review and approve or disapprove all Site Security Plans that satisfy the requirements of § 27.225, including Alternative Security Programs submitted pursuant to § 27.235.

(i) The Department will review Site Security Plans through a two-step process. Upon receipt of Site Security Plan from the covered facility, the Department will

review the documentation and make a preliminary determination as to whether it satisfies the requirements of § 27.225. If the Department finds that the requirements are satisfied, the Department will issue a Letter of Authorization to the covered facility.

(ii) Following issuance of the Letter of Authorization, the Department will inspect the covered facility in accordance with § 27.250 for purposes of determining compliance with the requirements of this Part.

(iii) If the Department approves the Site Security Plan in accordance with § 27.250, the Department will issue a Letter of Approval to the facility, and the facility shall implement the approved Site Security Plan.

(2) The Department will not disapprove a Site Security Plan submitted under this Part based on the presence or absence of a particular security measure. The Department may disapprove a Site Security Plan that fails to satisfy the risk-based performance standards established in § 27.230.

(b) When the Department disapproves a preliminary Site Security Plan issued prior to inspection or a Site Security Plan following inspection, the Department will provide the facility with a written notification that includes a clear explanation of deficiencies in the Site Security Plan. The facility shall then enter further consultations with the Department and resubmit a sufficient Site Security Plan by the time specified in the written notification provided by the Department under this section. If the resubmitted Site Security Plan does not satisfy the requirements of § 27.225, the Department will provide the facility with written notification (including a clear explanation of deficiencies in the SSP) of the Department's disapproval of the SSP.

§ 27.250 Inspections and audits.

(a) Authority. In order to assess compliance with the requirements of this Part, authorized Department officials may enter, inspect, and audit the property, equipment, operations, and records of covered facilities.

(b) Following preliminary approval of a Site Security Plan in accordance with § 27.245, the Department will inspect the covered facility for purposes of determining compliance with the requirements of this Part.

(1) If after the inspection, the Department determines that the requirements of § 27.225 have been met, the Department will issue a Letter of Approval to the covered facility.

(2) If after the inspection, the Department determines that the requirements of § 27.225 have not been met, the Department will proceed as directed by § 27.245(b) in "Review and Approval of Site Security Plans."

(c) Time and Manner. Authorized Department officials will conduct audits and inspections at reasonable times and in a reasonable manner. The Department will provide covered facility owners and/or operators with 24-hour advance notice before inspections, except

(1) if the Under Secretary or Assistant Secretary determines that an inspection without such notice is warranted by exigent circumstances and approves such inspection; or

(2) if any delay in conducting an inspection might be seriously detrimental to security, and the Director of the Chemical Security Division determines that an

inspection without notice is warranted, and approves an inspector to conduct such inspection.

(d) Inspectors. Inspections and audits are conducted by personnel duly authorized and designated for that purpose as "inspectors" by the Secretary or the Secretary's designee.

(1) An inspector will, on request, present his or her credentials for examination, but the credentials may not be reproduced by the facility.

(2) An inspector may administer oaths and receive affirmations, with the consent of any witness, in any matter.

(3) An inspector may gather information by reasonable means including, but not limited to, interviews, statements, photocopying, photography, and video- and audio-recording. All documents, objects and electronically stored information collected by each inspector during the performance of that inspector's duties shall be maintained for a reasonable period of time in the files of the Department of Homeland Security maintained for that facility or matter.

(4) An inspector may request forthwith access to all records required to be kept pursuant to § 27.255. An inspector shall be provided with the immediate use of any photocopier or other equipment necessary to copy any such record. If copies can not be provided immediately upon request, the inspector shall be permitted immediately to take the original records for duplication and prompt return.

(e) Confidentiality. In addition to the protections provided under CVI in §27.400, information received in an audit or inspection under this section, including the identity of the persons involved in the inspection or who provide information during the inspection,

shall remain confidential under the investigatory file exception, or other appropriate exception, to the public disclosure requirements of 5 U.S.C. 552.

(f) Guidance. The Assistant Secretary shall issue guidance identifying appropriate processes for such inspections, and specifying the type and nature of documentation that must be made available for review during inspections and audits.

§ 27.255 Recordkeeping requirements.

(a) Except as provided in § 27.255(b), the covered facility must keep records of the activities as set out below for at least three years and make them available to the Department upon request. A covered facility must keep the following records:

(1) Training. For training, the date and location of each session, time of day and duration of session, a description of the training, the name and qualifications of the instructor, a clear, legible list of attendees to include the attendee signature, at least one other unique identifier of each attendee receiving the training, and the results of any evaluation or testing.

(2) Drills and exercises. For each drill or exercise, the date held, a description of the drill or exercise, a list of participants, a list of equipment (other than personal equipment) tested or employed in the exercise, the name(s) and qualifications of the exercise director, and any best practices or lessons learned which may improve the Site Security Plan;

(3) Incidents and breaches of security. Date and time of occurrence, location within the facility, a description of the incident or breach, the identity of the individual to whom it was reported, and a description of the response;

(4) Maintenance, calibration, and testing of security equipment. The date and time, name and qualifications of the technician(s) doing the work, and the specific security equipment involved for each occurrence of maintenance, calibration, and testing;

(5) Security threats. Date and time of occurrence, how the threat was communicated, who received or identified the threat, a description of the threat, to whom it was reported, and a description of the response;

(6) Audits. For each audit of a covered facility's Site Security Plan (including each audit required under § 27.225(e)) or Security Vulnerability Assessment, a record of the audit, including the date of the audit, results of the audit, name(s) of the person(s) who conducted the audit, and a letter certified by the covered facility stating the date the audit was conducted.

(7) Letters of Authorization and Approval. All Letters of Authorization and Approval from the Department, and documentation identifying the results of audits and inspections conducted pursuant to § 27.250.

(b) A covered facility must retain records of submitted Top-Screens, Security Vulnerability Assessments, Site Security Plans, and all related correspondence with the Department for at least six years and make them available to the Department upon request.

(c) To the extent necessary for security purposes, the Department may request that a covered facility make available records kept pursuant to other Federal programs or regulations.

(d) Records required by this section may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized access, deletion, destruction, amendment, and disclosure.

Subpart C—Orders and Adjudications

§ 27.300 Orders.

(a) Orders Generally. When the Assistant Secretary determines that a facility is in violation of any of the requirements of this Part, the Assistant Secretary may take appropriate action including the issuance of an appropriate Order.

(b) Orders Assessing Civil Penalty and Orders to Cease Operations.

(1) Where the Assistant Secretary determines that a facility is in violation of an Order issued pursuant to paragraph (a), the Assistant may enter an Order Assessing Civil Penalty, Order to Cease Operations, or both.

(2) Following the issuance of an Order by the Assistant Secretary pursuant to paragraph (b)(1), the facility may enter further consultations with Department.

(3) Where the Assistant Secretary determines that a facility is in violation of an Order issued pursuant to paragraph (a) and issues an Order Assessing Civil Penalty pursuant to paragraph (b)(1), a chemical facility is liable to the United States for a civil penalty of not more than $25,000 for each day during which the violation continues.

(c) Procedures for Orders.

(1) At a minimum, an Order shall be signed by the Assistant Secretary, shall be dated, and shall include:

(i) The name and address of the facility in question;

(ii) A listing of the provision(s) that the facility is alleged to have violated;

(iii) A statement of facts upon which the alleged instances of noncompliance are based;

(iv) A clear explanation of deficiencies in the facility's chemical security program, including, if applicable, any deficiencies in the facility's Security Vulnerability Assessment, Site Security Plan, or both; and

(v) A statement, indicating what action(s) the chemical must take to remedy the instance(s) of noncompliance; and

(vi) The date by which the facility must comply with the terms of the Order.

(2) The Assistant Secretary may establish procedures for the issuance of Orders.

(d) A facility must comply with the terms of the Order by the date specified in the Order unless the facility has filed a timely Notice for Application for Review under § 27.310.

(e) Where a facility or other person contests the determination of the Assistant Secretary to issue an Order, a chemical facility may seek an adjudication pursuant to § 27.310.

(f) An Order issued under this section becomes final agency action when the time to file a Notice of Application of Review under § 27.310 has passed without such a filing or upon the conclusion of adjudication or appeal proceedings under this subpart.

§ 27.305 Neutral adjudications.

(a) Any facility or other person who has received a Finding pursuant to § 27.230(12)(iv), a Determination pursuant to § 27.245(b), or an Order pursuant to § 27.300 is entitled to an adjudication, by a neutral adjudications officer, of any issue of material fact relevant to any administrative action which deprives that person of a cognizable interest in liberty or property.

(b) A neutral adjudications officer appointed pursuant to § 27.315 shall issue an Initial Decision on any material factual issue related to a Finding pursuant to § 27.230(12)(iv), a Determination pursuant to § 27.245, or an Order pursuant to § 27.300 before any such administrative action is reviewed on appeal pursuant to § 27.345.

§ 27.310 Commencement of adjudication proceedings.

(a) Proceedings Instituted by Facilities or other Persons. A facility or other person may institute proceedings to review a determination by the Assistant Secretary:

(1) Finding, pursuant to the § 27.230(12)(iv), that an individual is a potential security threat;

(2) Disapproving a Site Security Plan pursuant to § 27.245(b); or

(3) Issuing an Order pursuant to § 27.300(a) or (b).

(b) Procedure for Applications by Facilities or other Persons A facility or other person may institute Proceedings by filing a Notice of Application for Review specifying that the facility or other person requests a Proceeding to review a determination specified in subpart (a).

(1) An Applicant institutes a Proceeding by filing a Notice of Application for Review with the office of the Department hereinafter designated by the Secretary.

(2) An Applicant must file a Notice of Application for Review within seven calendar days of notification to the facility or other person of the Assistant Secretary's Finding, Determination, or Order.

(3) The Applicant shall file and simultaneously serve each Notice of Application for Review and all subsequent filings on the Assistant Secretary and the General Counsel.

(4) An Order is stayed from the timely filing of a Notice of Application for Review until the Presiding Officer issues an Initial Decision, unless the Secretary has lifted the stay due to exigent circumstances pursuant to paragraph (d).

(5) The Applicant shall file and serve an Application for Review within fourteen calendar days of the notification to the facility or other person of the Assistant Secretary's Finding, Determination, or Order.

(6) Each Application for Review shall be accompanied by all legal memoranda, other documents, declarations, affidavits, and other evidence supporting the position asserted by the Applicant.

(c) Response The Assistant Secretary, through the Office of General Counsel, shall file and serve a Response, accompanied by all legal memoranda, other documents, declarations, affidavits and other evidence supporting the position asserted by the Assistant Secretary within fourteen calendar days of the filing and service of the Application for Review and all supporting papers.

(d) Procedural Modifications The Secretary may, in exigent circumstances (as determined in his sole discretion):

(i) lift any stay applicable to any Order under § 27.300;

(ii) modify the time for a response;

(iii) rule on the sufficiency of Applications for Review; or

(iv) otherwise modify these procedures with respect to particular matters.

§27.315 Presiding officers for proceedings.

(a) Immediately upon the filing of any Application for Review, the Secretary shall appoint an attorney, who is employed by the Department and who has not performed any investigative or prosecutorial function with respect to the matter, to act as a neutral adjudications officer or Presiding Officer for the compilation of a factual record and the recommendation of an Initial Decision for each Proceeding.

(b) Notwithstanding paragraph (a), the Secretary may appoint one or more attorneys who are employed by the Department and who do not perform any investigative or prosecutorial function with respect to this subpart, to serve generally in the capacity as Presiding Officer(s) for such matters pursuant to such procedures as the Secretary may hereafter establish.

§ 27.320 Prohibition on ex parte communications during proceedings.

(a) At no time after the designation of a Presiding Officer for a Proceeding and prior to the issuance of a Final Decision pursuant to § 27.345 with respect to a facility or other person, shall the appointed Presiding Officer, or any person who will advise that

official in the decision on the matter, discuss *ex parte* the merits of the proceeding with any interested person outside the Department, with any Department official who performs a prosecutorial or investigative function in such proceeding or a factually related proceeding, or with any representative of such person.

(b) If, after appointment of a Presiding Officer and prior to the issuance of a Final Decision pursuant to § 27.345 with respect to a facility or other person, the appointed Presiding Officer, or any person who will advise that official in the decision on the matter, receives from or on behalf of any party, by means of an *ex parte* communication, information which is relevant to the decision of the matter and to which other parties have not had an opportunity to respond, a summary of such information shall be served on all other parties, who shall have an opportunity to reply to the *ex parte* communication within a time set by the Presiding Officer.

(c) The consideration of classified information or CVI pursuant to an in camera procedure does not constitute a prohibited ex parte communication for purposes of this subpart.

§ 27.325 Burden of proof.

The Assistant Secretary bears the initial burden of proving the facts necessary to support the challenged administrative action at every proceeding instituted under this subpart.

§ 27.330 Summary decision procedures.

(a) The Presiding Officer appointed for each Proceeding shall immediately consider whether the summary adjudication of the Application for Review is appropriate based on the Application for Review, the Response, and all the supporting filings of the parties pursuant to §§ 27.310(b)(5) and 27.310(c).

(1) The Presiding Officer shall promptly issue any necessary scheduling order for any additional briefing of the issue of summary adjudication on the Application for Review and Response.

(2) The Presiding Officer may conduct scheduling conferences and other proceedings that the Presiding Officer determines to be appropriate.

(b) If the Presiding Officer determines that there is no genuine issue of material fact and that one party or the other is entitled to decision as a matter of law, then the record shall be closed and the Presiding Officer shall issue an Initial Decision on the Application for Review pursuant to § 27.340.

(c) If a Presiding Officer determines that any factual issues require the cross-examination of one or more witnesses or other proceedings at a hearing, the Presiding Officer, in consultation with the parties, shall promptly schedule a hearing to be conducted pursuant to § 27.335.

§ 27.335 Hearing procedures.

(a) Any hearing shall be held as expeditiously as possible at the location most conducive to a prompt presentation of any necessary testimony or other proceedings.

(1) Videoconferencing and teleconferencing may be used where appropriate at the discretion of the Presiding Officer.

(2) Each party offering the affirmative testimony of a witness shall present that testimony by declaration, affidavit, or other sworn statement submitted in advance as ordered by the Presiding Officer.

(3) Any witness presented for further examination shall be asked to testify under an oath or affirmation.

(4) The hearing shall be recorded verbatim.

(b)(1) A facility or other person may appear and be heard on his own behalf or through any counsel of his choice who is qualified to possess CVI.

(2) A facility of other person individually, or through counsel, may offer relevant and material information including written direct testimony which he believes should be considered in opposition to the administrative action or which may bear on the sanction being sought.

(3) The facility or other person individually, or through counsel, may conduct such cross-examination as may be specifically allowed by the Presiding Officer for a full determination of the facts.

§ 27.340 Completion of adjudication proceedings.

(a) The Presiding Officer shall close and certify the record of the adjudication promptly upon the completion of:

(1) summary judgment proceedings,

(2) a hearing, if necessary,

(3) the submission of post hearing briefs, if any are ordered by the Presiding Officer, and

(4) the conclusion of oral arguments, if any are permitted by the Presiding Officer.

(b) The Presiding Officer shall issue an Initial Decision based on the certified record, and the decision shall be subject to appeal pursuant to § 27.345.

(c) An Initial Decision shall become a final agency action on the expiration of the time for an Appeal pursuant to § 27.345.

§ 27.345 Appeals.

(a) Right to Appeal. A facility or any person who has received an Initial Decision under § 27.340(b) has the right to appeal to the Under Secretary acting as a neutral appeals officer.

(b) Procedure for Appeals.

(1) The Assistant Secretary, a facility or other person, or a representative on behalf of a facility or person, may institute an Appeal by filing a Notice of Appeal with the office of the Department hereinafter designated by the Secretary.

(2) The Assistant Secretary, a facility, or other person must file a Notice of Appeal within seven calendar days of the service of the Presiding Officer's Initial Decision.

(3) The Appellant shall file with the designated office and simultaneously serve each Notice of Appeal and all subsequent filings on the General Counsel.

(4) An Initial Decision is stayed from the timely filing of a Notice of Appeal until the Under Secretary issues a Final Decision, unless the Secretary lifts the stay due to exigent circumstances pursuant to §27.310(d).

(5) The Appellant shall file and serve a Brief within 28 calendar days of the notification of the service of the Presiding Officer's Initial Decision.

(6) The Appellee shall file and serve its Opposition Brief within 28 calendar days of the service of the Appellant's Brief.

(c) The Under Secretary may provide for an expedited appeal for appropriate matters.

(d) Ex Parte Communications.

(1) At no time after the filing of a Notice of Appeal pursuant to paragraph (b)(1) and prior to the issuance of a Final Decision on an Appeal pursuant to paragraph (f) with respect to a facility or other person shall the Under Secretary, his designee, or any person who will advise that official in the decision on the matter, discuss *ex parte* the merits of the proceeding with any interested person outside the Department, with any Department official who performs a prosecutorial or investigative function in such proceeding or a factually related proceeding, or with any representative of such person.

(2) If, after the filing of a Notice of Appeal pursuant to paragraph (b)(1) and prior to the issuance of a Final Decision on an Appeal pursuant to paragraph (f) with respect to a facility or other person, the Under Secretary, his designee, or any person who will advise that official in the decision on the matter, receives from or on behalf of any party, by means of an *ex parte* communication, information which is relevant to the decision of the matter and to which other parties have not had an opportunity to respond, a summary of such information shall be served on all other parties, who shall have an opportunity to reply to the *ex parte* communication within a time set by the Under Secretary or his designee.

(3) The consideration of classified information or CVI pursuant to an in camera procedure does not constitute a prohibited ex parte communication for purposes of this subpart.

(e) A facility or other person may elect to have the Under Secretary participate in any mediation or other resolution process by expressly waiving, in writing, any argument that such participation has compromised the Appeal process.

(f) The Under Secretary shall issue a Final Decision and serve it upon the parties. A Final Decision made by the Under Secretary constitutes final agency action.

(g) The Secretary may establish procedures for the conduct of Appeals pursuant to this section.

Subpart D—Other

§ 27.400 Chemical-terrorism vulnerability information.

(a) Applicability. This section governs the maintenance, safeguarding, and disclosure of information and records that constitute Chemical-terrorism Vulnerability Information (CVI), as defined in § 27.400(b). The Secretary shall administer this section consistent with Section 550(c) of the Homeland Security Appropriations Act of 2007, including appropriate sharing with Federal, State and local officials.

(b) Chemical-terrorism Vulnerability Information. In accordance with Section 550(c) of the Department of Homeland Security Appropriations Act of 2007, the following information, whether transmitted verbally, electronically, or in written form, shall constitute CVI:

(1) Security Vulnerability Assessments under § 27.215;

(2) Site Security Plans under § 27.225;

(3) Documents relating to the Department's review and approval of Security Vulnerability Assessments and Site Security Plans, including Letters of Authorization, Letters of Approval and responses thereto; written notices; and other documents developed pursuant to §§ 27.240 or 27.245;

(4) Alternate Security Programs under § 27.235;

(5) Documents relating to inspection or audits under § 27.250;

(6) Any records required to be created or retained under § 27.255;

(7) Sensitive portions of orders, notices or letters under § 27.300;

(8) Information developed pursuant to §§ 27.200 and 27.205; and

(9) Other information developed for chemical facility security purposes that the Secretary, in his discretion, determines is similar to the information protected in sections § 27.400(b)(1)-(8) and thus warrants protection as CVI.

(c) Covered Persons. Persons subject to the requirements of this section are:

(1) Each person who has a need to know CVI, as specified in § 27.400(e);

(2) Each person who otherwise receives or gains access to what they know or should reasonably know constitutes CVI.

(d) Duty to protect information. A covered person must--

(1) Take reasonable steps to safeguard CVI in that person's possession or control, including electronic data, from unauthorized disclosure. When a person is not in physical possession of CVI, the person must store it a secure container, such as a safe, that limits access only to covered persons with a need to know;

(2) Disclose, or otherwise provide access to, CVI only to persons who have a need to know;

(3) Refer requests for CVI by persons without a need to know to the Assistant Secretary;

(4) Mark CVI as specified in § 27.400(f);

(5) Dispose of CVI as specified in § 27.400(k);

(6) If a covered person receives a record or verbal transmission containing CVI that is not marked as specified in § 27.400(f), the covered person must--

(i) Mark the record as specified in § 27.400(f) of this section; and

(ii) Inform the sender of the record that the record must be marked as specified in § 27.400(f); or

(iii) If received verbally, make reasonable efforts to memorialize such information and mark the memorialized record as specified in § 27.400(f) of this section, and inform the speaker of any determination that such information warrants CVI protection.

(7) When a covered person becomes aware that CVI has been released to persons without a need to know (including a covered person under § 27.400(c)(2)), the covered person must promptly inform the Assistant Secretary.

(8) In the case of information that is CVI and also has been designated as critical infrastructure information under Section 214 of the Homeland Security Act, any covered person in possession of such information must comply with the disclosure restrictions and other requirements applicable to such information under Section 214 and any implementing regulations.

(e) Need to know.

(1) A person, including a State or local official, has a need to know CVI in each of the following circumstances:

(i) When the person requires access to specific CVI to carry out chemical facility security activities approved, accepted, funded, recommended, or directed by the Department.

(ii) When the person needs the information to receive training to carry out chemical facility security activities approved, accepted, funded, recommended, or directed by the Department.

(iii) When the information is necessary for the person to supervise or otherwise manage individuals carrying out chemical facility security activities approved, accepted, funded, recommended, or directed by the Department.

(iv) When the person needs the information to provide technical or legal advice to a covered person, who has a need to know the information, regarding chemical facility security requirements of Federal law.

(v) When the Department determines that access is required under §§ 27.400(h) or 27.400(i) in the course of a judicial or administrative proceeding.

(2) Federal employees, contractors, and grantees.

(i) A Federal employee has a need to know CVI if access to the information is necessary for performance of the employee's official duties.

(ii) A person acting in the performance of a contract with or grant from the Department has a need to know CVI if access to the information is necessary to

performance of the contract or grant. Contractors or grantees may not further disclose CVI without the consent of the Assistant Secretary.

(iii) The Department may require that non-Federal persons seeking access to CVI complete a non-disclosure agreement before such access is granted.

(3) Background check. The Department may make an individual's access to the CVI contingent upon satisfactory completion of a security background check or other procedures and requirements for safeguarding CVI that are satisfactory to the Department.

(4) Need to know further limited by the Department. For some specific CVI, the Department may make a finding that only specific persons or classes of persons have a need to know.

(5) Nothing in § 27.400(e) shall prevent the Department from determining, in its discretion, that a person not otherwise listed in § 27.400(e) has a need to know CVI in a particular circumstance.

(f) Marking of paper records.

(1) In the case of paper records containing CVI, a covered person must mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of--

(i) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover;

(ii) Any title page; and

(iii) Each page of the document.

(2) Protective marking. The protective marking is: CHEMICAL-

TERRORISM VULNERABILITY INFORMATION.

(3) Distribution limitation statement. The distribution limitation statement is: WARNING: This record contains Chemical-terrorism Vulnerability Information controlled by 6 CFR 27.400. Do not disclose to persons without a "need to know" in accordance with 6 CFR § 27.400(e). Unauthorized release may result in civil penalties or other action. In any administrative or judicial proceeding, this information shall be treated as classified information in accordance with 6 CFR §§ 27.400(h) and (i).

(4) Other types of records. In the case of non-paper records that contain CVI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.

(g) Disclosure by the Department --In general.

(1) Except as otherwise provided in this section, and notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, records containing CVI are not available for public inspection or copying, nor does the Department release such records to persons without a need to know.

(2) Disclosure of Segregatable Information under the Freedom of Information Act and the Privacy Act. If a record is marked to signify both CVI and information that is not CVI, the Department, on a proper Freedom of Information Act or Privacy Act request, may disclose the record with the CVI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act.

(h) Disclosure in administrative enforcement proceedings.

(1) The Department may provide CVI to a person governed by Section 550, and his counsel, in the context of an administrative enforcement proceeding of Section 550 when, in the sole discretion of the Department, as appropriate, access to the CVI is necessary for the person to prepare a response to allegations contained in a legal enforcement action document issued by the Department.

(2) Security background check. Prior to providing CVI to a person under § 27.400(h)(1), the Department may require the individual or, in the case of an entity, the individuals representing the entity, and their counsel, to undergo and satisfy, in the judgment of the Department, a security background check.

(i) Disclosure in judicial proceedings.

(1) In any judicial enforcement proceeding of Section 550, the Secretary, in his sole discretion, may, subject to § 27.400(i)(1)(A), authorize access to CVI for persons necessary for the conduct of such proceedings, including such persons' counsel, provided that no other persons not so authorized shall have access to or be present for the disclosure of such information.

(i) Security background check. Prior to providing CVI to a person under § 27.400(i)(1), the Department may require the individual to undergo and satisfy, in the judgment of the Department, a security background check.

(2) In any judicial enforcement proceeding of Section 550 where a person seeks to disclose CVI to a person not authorized to receive it under paragraph (i)(1), or where a person not authorized to receive CVI under paragraph (i)(1) seeks to compel its

disclosure through discovery, the United States may make an ex parte application in writing to the court seeking authorization to--

(i) Redact specified items of CVI from documents to be introduced into evidence or made available to the defendant through discovery under the Federal Rules of Civil Procedure;

(ii) Substitute a summary of the information for such CVI; or

(iii) Substitute a statement admitting relevant facts that the CVI would tend to prove.

(3) The court shall grant a request under paragraph (i)(2) of this section if, after in camera review, the court finds that the redacted item, stipulation, or summary is sufficient to allow the defendant to prepare a defense.

(4) If the court enters an order granting a request under paragraph (i)(2) of this section, the entire text of the documents to which the request relates shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.

(5) If the court enters an order denying a request of the United States under paragraph (b)(i)(2) of this section, the United States may take an immediate, interlocutory appeal of the court's order in accordance with 18 U.S.C. 2339B(f)(4), (5). For purposes of such an appeal, the entire text of the documents to which the request relates, together with any transcripts of arguments made ex parte to the court in connection therewith, shall be maintained under seal and delivered to the appellate court.

(6) Except as provided otherwise at the sole discretion of the Secretary, access to CVI shall not be available in any civil or criminal litigation unrelated to the enforcement of Section 550.

(7) Taking of trial testimony--

(i) Objection--During the examination of a witness in any judicial proceeding, the United States may object to any question or line of inquiry that may require the witness to disclose CVI not previously found to be admissible.

(ii) Action by court--In determining whether a response is admissible, the court shall take precautions to guard against the compromise of any CVI, including--

(A) Permitting the United States to provide the court, ex parte, with a proffer of the witness's response to the question or line of inquiry; and

(B) Requiring the defendant to provide the court with a proffer of the nature of the information that the defendant seeks to elicit.

(iii) Obligation of defendant--In any judicial enforcement proceeding, it shall be the defendant's obligation to establish the relevance and materiality of any CVI sought to be introduced.

(8) Construction. Nothing in this subsection shall prevent the United States from seeking protective orders or asserting privileges ordinarily available to the United States to protect against the disclosure of classified information, including the invocation of the military and State secrets privilege.

(j) Consequences of Violation. Violation of this section is grounds for a civil penalty and other enforcement or corrective action by the Department, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an

order requiring retrieval of CVI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

(k) Destruction of CVI.

(1) The Department of Homeland Security. Subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve records containing documentation of a Federal agency's policies, decisions, and essential transactions, the Department destroys CVI when no longer needed to carry out the agency's function.

(2) Other covered persons.

(i) In general. A covered person must destroy CVI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the CVI to carry out security measures under paragraph (e) of this section.

(ii) Exception. Section 27.400(k)(2) does not require a State or local government agency to destroy information that the agency is required to preserve under State or local law.

§ 27.405 Review and preemption of State laws and regulations.

(a) As per current law, no law, regulation, or administrative action of a State or political subdivision thereof, or any decision or order rendered by a court under state law, shall have any effect if such law, regulation, or decision conflicts with, hinders, poses an obstacle to or frustrates the purposes of this regulation or of any approval, disapproval or order issued there under.

(1) Nothing in this regulation is intended to displace other federal requirements administered by the Environmental Protection Agency, U.S. Department of Justice, U.S. Department of Labor, U.S. Department of Transportation, or other federal agencies.

(2) [Reserved]

(b) State law, regulation or administrative action defined. For purposes of this section, the phrase "State law, regulation or administrative action" means any enacted law, promulgated regulation, ordinance, administrative action, order or decision, or common law standard of a State or any of its political subdivisions.

(c) Submission for review. Any chemical facility covered by these regulations and any State may petition the Department by submitting a copy of a State law, regulation, or administrative action, or decision or order of a court for review under this section.

(d) Review and opinion.

(1) Review. The Department may review State laws, administrative actions, or opinions or orders of a court under State law and regulations submitted under this section, and may offer an opinion whether the application or enforcement of the State law or regulation would conflict with, hinder, pose an obstacle to or frustrate the purposes of this Part.

(2) Opinion. The Department may issue a written opinion on any question regarding preemption. If the question was submitted under subsection (c) of this part, the Assistant Secretary will notify the affected chemical facility and the Attorney General of the subject State of any opinion under this section.

(3) Consultation with States. In conducting a review under this section, the Department will seek the views of the State or local jurisdiction whose laws may be affected by the Department's review.

§ 27.410 Third party actions.

(a) Nothing in this Part shall confer upon any person except the Secretary a right of action, in law or equity, for any remedy including, but not limited to, injunctions or damages to enforce any provision of this Part.

(b) An owner or operator of a chemical facility may petition the Assistant Secretary to provide the Department's view in any litigation involving any issues or matters regarding this Part.

Proposed Appendix A: DHS Chemicals of Interest

Chemical of Interest	Chemical Abstract Service (CAS) Number	Screening Threshold Quantity (STQ) (lbs)
1,1,3,3,3-pentafluoro-2-(trifluoromethyl)-1-propene	382-21-8	Any Amount
1,1-Dimethylhydrazine	57-14-7	11,250
1,2-bis(2-chloroethylthio)ethane	3563-36-8	Any Amount
1,3-bis(2-chloroethylthio)-n-propane	63905-10-2	Any Amount
1,3-Butadiene	106-99-0	7,500
1,3-Pentadiene	504-60-9	7,500
1,4-bis(2-chloroethylthio)-n-butane	142868-93-7	Any Amount
1,5-bis(2-chloroethylthio)-n-pentane	142868-94-8	Any Amount
1-Butene	106-98-9	7,500
1-Chloropropylene	590-21-6	7,500
1H-Tetrazole	16681-77-9	2,000
1-Pentane	109-67-1	7,500
2,2-Dimethylpropane	463-82-1	7,500
2-Butene	107-01-7	7,500
2-Butene-cis	590-18-1	7,500
2-Butene-trans	624-64-6	7,500
2-chloroethylchloromethylsulfide	2625-76-5	Any Amount
2-Chloropropylene	557-98-2	7,500
2-Chlorovinyldichloroarsine	541-25-3	Any Amount
2-Methyl-1-butene	563-46-2	7,500
2-Methylpropene	115-11-7	7,500
2-Pentene, (Z)-	627-20-3	7,500
2-Pentene,(E)-	646-04-8	7,500
3,3-dimethyl-2-butanol	464-07-3	Any Amount
3-Methyl-1-butene	563-45-1	7,500
3-Quinuclidinyl benzilate (BZ)	62869-69-6	Any Amount
5-Nitrobenzotriazol	2338-12-7	2,000
Acetaldehyde	75-07-0	7,500
Acetone	67-64-1	2,000
Acetone cyanohydrin, stabilized	75-86-5	2,000
Acetyl bromide	506-96-7	2,000
Acetyl chloride	75-36-5	2,000
Acetyl iodide	507-02-8	2,000
Acetylene	74-86-2	7,500
Acrolein	107-02-8	3,750
Acrylonitrile	107-13-1	15,000
Acrylyl chloride	814-68-6	3,750

Allyl alcohol	107-18-6	11,250
Allylamine	107-11-9	7,500
Allyltrichlorosilane, stabilized	107-37-9	2,000
Aluminum bromide, anhydrous	7727-15-3	2,000
Aluminum chloride, anhydrous	7446-70-0	2,000
Aluminum phosphide	20859-73-8	2,000
Ammonia (anhydrous)	7664-41-7	7,500
Ammonia (conc. 20% or greater)	7664-41-7	15,000
Ammonium nitrate (nitrogen concentration of 28%-34%)	6484-52-2	2,000
Ammonium perchlorate	7790-98-9	2,000
Ammonium picrate	131-74-8	2,000
Amyltrichlorosilane	107-72-2	2,000
Antimony pentafluoride	7783-70-2	2,000
Arsenous trichloride	7784-34-1	Any Amount
Arsine	7784-42-1	Any Amount
Barium azide	18810-58-7	2,000
bis(2-chloroethyl)ethylamine	538-07-8	Any Amount
bis(2-chloroethyl)methylamine	51-75-2	Any Amount
bis(2-chloroethyl)sulfide	505-60-2	Any Amount
bis(2-chloroethylthio)methane	63869-13-6	Any Amount
bis(2-chloroethylthioethyl)ether	63918-89-8	Any Amount
bis(2-chloroethylthiomethyl)ether	63918-90-1	Any Amount
bis(2-chlorovinyl)chloroarsine	40334-69-8	Any Amount
Boron tribromide	10294-33-4	2,000
Boron trichloride	10294-34-5	Any Amount
Boron triflouride	7637-07-2	Any Amount
Boron triflouride compound with methyl ether (1:1)	353-42-4	11,250
Bromine	7726-95-6	7,500
Bromine chloride	13863-41-7	Any Amount
Bromine pentafluoride	7789-30-2	2,000
Bromine trifluoride	7787-71-5	2,000
Bromotrifluorethylene	598-73-2	7,500
Butane	106-97-8	7,500
Butene	25167-67-3	7,500
Butyltrichlorosilane	7521-80-4	2,000
Calcium dithionite	15512-36-4	2,000
Calcium hydrosulfite	15512-36-4	2,000
Calcium phosphide	1305-99-3	2,000
Carbon disulfide	75-15-0	15,000
Carbon monoxide	630-08-0	Any Amount
Carbon oxysulfide	463-58-1	7,500
Carbonyl fluoride	353-50-4	Any Amount
Carbonyl sulfide	463-58-1	Any Amount
Chlorine	7782-50-5	1,875

Chlorine dioxide	10049-04-4	2,000
Chlorine monoxide	7791-21-1	7,500
Chlorine pentafluoride	13637-63-3	Any Amount
Chlorine trifluoride	7790-91-2	Any Amount
Chloroacetyl chloride	79-04-9	2,000
Chloroform	67-66-3	15,000
Chloromethyl ether	542-88-1	750
Chloromethyl methyl ether	107-30-2	3,750
Chloropicrin	76-06-2	Any Amount
Chlorosulfonic acid	7790-94-5	2,000
Chromium oxychloride	7803-51-2	2,000
Crotonaldehyde	4170-30-3	15,000
Crotonaldehyde, (E)-	123-73-9	15,000
Cyanogen	460-19-5	Any Amount
Cyanogen chloride	506-77-4	Any Amount
Cyclohexylamine	108-91-8	11,250
Cyclohexyltrichlorosilane	98-12-4	2,000
Cyclopropane	75-19-4	7,500
Cyclotetramethylenetetranitramine	2691-41-0	2,000
Diazodinitrophenol	87-31-0	2,000
Diborane	19287-45-7	Any Amount
Dichlorosilane	4109-96-0	Any Amount
Diethyl ethylphosphonate	78-38-6	Any Amount
Diethyl N,N-dimethylphosphoramidate	2404-03-7	Any Amount
Diethyl phosphate	762-04-9	Any Amount
Diethyldichlorosilane	1719-53-5	2,000
Diethyleneglycol dinitrate,	693-21-0	2,000
Difluoroethane	75-37-6	7,500
Dimethyl ethylphosphonate	6163-75-3	Any Amount
Dimethyl methylphosphonate	756-79-6	Any Amount
Dimethyl phosphate	868-85-9	Any Amount
Dimethylamine	124-40-3	7,500
Dimethyldichlorosilane	75-78-5	2,000
Dimethylphosphoramidodichloridate	677-43-0	Any Amount
Dinitrogen tetroxide	10544-72-6	Any Amount
Dinitroglycoluril	55510-04-8	2,000
Dinitrophenol	25550-58-7	2,000
Dinitroresorcinol	35860-51-6	2,000
Dinitrosobenzene	25550-55-4	2,000
Diphenyl-2-hydroxyacetic acid (aka benzilic acid)	76-93-7	Any Amount
Diphenyldichlorosilane	80-10-4	2,000
Dipicryl sulfide	2217-06-3	2,000
Dodecyltrichlorosilane	4484-72-4	2,000
Epichlorohydrin	106-89-8	15,000
Ethane	74-84-0	7,500

Ethyl acetylene	107-00-6	7,500
Ethyl chloride	75-00-3	7,500
Ethyl ether	60-29-7	7,500
Ethyl mercaptan	75-08-1	7,500
Ethyl nitrite	109-95-5	7,500
Ethyl phosphonyl dichloride	1066-50-8	Any Amount
Ethyl phosphonyl difluoride	753-98-0	Any Amount
Ethylamine	75-04-7	7,500
Ethyldiethanolamine	139-87-7	Any Amount
Ethylene	74-85-1	7,500
Ethylene oxide	75-21-8	Any Amount
Ethylenediamine	107-15-3	15,000
Ethyleneimine	151-56-4	7,500
Ethyltrichlorosilane	115-21-9	2,000
Fluorine	7782-41-4	Any Amount
Fluorosulfonic acid	7789-21-1	2,000
Formaldehyde (solution)	50-00-0	11,250
Furan	110-00-9	3,750
Germane	7782-65-2	Any Amount
Germanium tetrafluoride	7783-58-6	Any Amount
Guanyl nitrosaminoguanylidene hydrazine		2,000
Guanyl nitrosaminoguanyltetrazene	109-27-3	2,000
Hexaethyl tetraphosphate and compressed gas mixtures	757-58-4	Any Amount
Hexafluoroacetone	684-16-2	Any Amount
Hexanitrodiphenylamine	35860-31-2	2,000
Hexanitrostilbene	20062-22-0	2,000
Hexolite	121-82-4	2,000
Hexotonal	107-15-3	2,000
Hexyltrichlorosilane	928-89-2 6	2,000
Hydrazine	302-01-2	11,250
Hydrochloric acid (conc. 37% or greater)	7647-01-0	11,250
Hydrocyanic acid	74-90-8	1,875
Hydrogen	1333-74-0	7,500
Hydrogen bromide, anhydrous	10035-10-6	Any Amount
Hydrogen chloride (anhydrous)	7647-01-0	Any Amount
Hydrogen cyanide	74-90-8	Any Amount
Hydrogen fluoride/Hydrofluoric acid (conc. 50% or greater)	7664-39-3	750
Hydrogen iodide, anhydrous	10034-85-2	Any Amount
Hydrogen peroxide (concentration of at least 30%)	7722-84-1	2,000
Hydrogen selenide	7783-07-5	Any Amount
Hydrogen sulfide	7783-06-4	Any Amount
Iodine pentafluoride	7783-66-6	2,000
Iron, pentacarbonyl-	13463-40-6	1,875

Isobutane	75-28-5	7,500
Isobutyronitrile	78-82-0	15,000
Isopentane	78-78-4	7,500
Isoprene	78-79-5	7,500
Isopropyl chloride	75-29-6	7,500
Isopropyl chloroformate	108-23-6	11,250
Isopropylamine	75-31-0	7,500
Lead azide	13424-46-9	2,000
Lead styphnate	15245-44-0	2,000
Lithium amide	7782-89-0	2,000
Lithium nitride	26134-62-3	2,000
Magnesium aluminum phosphide		2,000
Magnesium diamide	7803-54-5	2,000
Magnesium phosphide	12057-74-8	2,000
Mannitol hexanitrate, wetted	15825-70-4	2,000
Mercury fulminate	628-86-4	2,000
Methacrylonitrile	126-98-7	7,500
Methane	74-82-8	7,500
Methyl bromide	74-83-9	Any Amount
Methyl chloride	74-87-3	7,500
Methyl chloroformate	79-22-1	3,750
Methyl ether	115-10-6	7,500
Methyl formate	107-31-3	7,500
Methyl hydrazine	60-34-4	11,250
Methyl isocyanate	624-83-9	11,250
Methyl mercaptan	74-93-1	Any Amount
Methyl phosphonyl dichloride	676-97-1	Any Amount
Methyl phosphonyl difluoride	676-99-3	Any Amount
Methyl thiocyanate	556-64-9	15,000
Methylamine	74-89-5	7,500
Methylchlorosilane	993-00-0	Any Amount
Methyldichlorosilane	75-54-7	2,000
Methyldiethanolamine	105-59-9	Any Amount
Methylphenyldichlorosilane	149-74-6	2,000
Methyltrichlorosilane	75-79-6	2,000
N,N-diisopropyl-2-aminoethyl chloride hydrochloride	4261-68-1	Any Amount
N,N-diisopropyl-β-aminoethanol	96-80-0	Any Amount
N,N-diisopropyl-β-aminoethyl chloride	96-79-7	Any Amount
Nickel Carbonyl	13463-39-3	750
Nitric acid	7697-37-2	2,000
Nitric oxide	10102-43-9	Any Amount
Nitro urea	556-89-8	2,000
Nitrocellulose	9004-70-0	2,000
Nitrogen trioxide	10544-73-7	Any Amount

Nitroglycerine	55-63-0	2,000
Nitroguanidine	556-88-7	2,000
Nitromethane	75-52-5	2,000
Nitrostarch	9056-38-6	2,000
Nitrosyl chloride	2696-92-6	Any Amount
Nitrotriazolone	932-64-9	2,000
Nonyltrichlorosilane	5283-67-0	2,000
o,o-diethyl S-[2-(diethylamino)ethyl] phosphorothiolate	78-53-5	Any Amount
Octadecyltrichlorosilane	112-04-9	2,000
Octolite	68610-51-5	2,000
Octonal	124-13-0	2,000
Octyltrichlorosilane	5283-66-9	2,000
o-ethyl-N,N-dimethylphosphoramido-cyanidate	77-81-6	Any Amount
o-ethyl-o-2-diisopropylaminoethyl methylphosphonite	57856-11-8	Any Amount
o-ethyl-S-2-diisopropylaminoethyl methyl phosphonothiolate	50782-69-9	Any Amount
o-isopropyl methylphosphonochloridate	1445-76-7	Any Amount
o-isopropyl methylphosphonofluoridate	107-44-8	Any Amount
Oleum (Fuming Sulfuric acid)	8014-95-7	7,500
o-pinacolyl methylphosphonochloridate	7040-57-5	Any Amount
o-pinacolyl methylphosphonofluoridate	96-64-0	Any Amount
Oxygen difluoride	7783-41-7	Any Amount
Pentaerythrite tetranitrate or PETN	78-11-5	2,000
Pentane	109-66-0	7,500
Pentolite	8066-33-9	2,000
Peracetic acid	79-21-0	7,500
Perchloromethylmercaptan	594-42-3	7,500
Perchloryl fluoride	7616-94-6	Any Amount
Phenyltrichlorosilane	98-13-5	2,000
Phosgene	75-44-5	Any Amount
Phosphine	7803-51-2	Any Amount
Phosphorus	7723-14-0	Any Amount
Phosphorus oxychloride	10025-87-3	Any Amount
Phosphorus oxychloride	10025-87-3	2,000
Phosphorus pentachloride	10026-13-8	Any Amount
Phosphorus pentachloride	10026-13-8	2,000
Phosphorus pentasulfide	1314-80-3	2,000
Phosphorus trichloride	7719-12-2	Any Amount
Phosphorus trichloride	7719-12-2	2,000
Piperidine	110-89-4	11,250
Potassium chlorate	3811-04-9	2,000
Potassium cyanide	151-50-8	2,000
Potassium nitrate	7757-79-1	2,000

Potassium perchlorate	7778-74-7	2,000
Potassium phosphide	20770-41-6	2,000
Propadiene	463-49-0	7,500
Propane	74-98-6	7,500
Propionitrile	107-12-0	7,500
Propyl chlorofromate	109-61-5	11,250
Propylene	115-07-1	7,500
Propylene oxide	75-56-9	7,500
Propyleneimine	75-55-8	7,500
Propyltrichlorosilane	141-57-1	2,000
Propyne	74-99-7	7,500
Quinuclidine-3-ol	1619-34-7	Any Amount
RDX and HMX mixtures	121-82-4	2,000
Selenium hexafluoride	7783-79-1	Any Amount
Silane	7803-62-5	7,500
Silicon tetrachloride	10026-04-7	2,000
Silicon tetrafluoride	7783-61-1	Any Amount
Sodium chlorate	7775-09-9	2,000
Sodium cyanide	143-33-9	2,000
Sodium dinitro-o-cresolate	25641-53-6	2,000
Sodium dithionite	7775-14-6	2,000
Sodium hydrosulfite	7775-14-6	2,000
Sodium nitrate	7631-99-4	2,000
Sodium phosphide	7558-80-7	2,000
Sodium picramate	831-52-7	2,000
Stibine	7803-52-3	Any Amount
Strontium phosphide	13450-99-2	2,000
Sulfur dichloride	10545-99-0	Any Amount
Sulfur dioxide (anhydrous)	7446-09-5	Any Amount
Sulfur monochloride	10025-67-9	Any Amount
Sulfur tetraflouride	7783-60-0	Any Amount
Sulfur trioxide	7446-11-9	7,500
Sulfuryl chloride	7791-25-5	2,000
Sulfuryl fluoride	2699-79-8	Any Amount
Tellurium hexafluoride	7783-80-4	Any Amount
Tetrafluoroethylene	116-14-3	7,500
Tetramethyllead	75-74-1	7,500
Tetramethylsilane	75-76-3	7,500
Tetranitroaniline	53014-37-2	2,000
Tetranitromethane	509-14-8	7,500
Tetrazol-1-acetic acid	21732-17-2	2,000
Thiodiglycol	111-48-8	Any Amount
Thionyl chloride	7719-09-7	Any Amount
Thionyl chloride	7719-09-7	2,000
Titanium tetrachloride	7550-45-0	2,000

Toluene 2,4-diisocyanate	584-84-9	7,500
Toluene 2,6-diisocyanate	91-08-7	7,500
Toluene diisocyanate (unspecified isomer)	26471-62-5	7,500
Trichlorosilane	10025-78-2	2,000
Triethanolamine	102-71-6	Any Amount
Triethanolamine hydrochloride	637-39-8	Any Amount
Triethyl phosphite	122-52-1	Any Amount
Trifluoroacetyl chloride	354-32-5	Any Amount
Trifluorochloroethylene	79-38-9	Any Amount
Trimethyl phosphite	121-45-9	Any Amount
Trimethylamine	75-50-3	Any Amount
Trimethylchlorosilane	75-77-4	2,000
Trinitroaniline	26952-42-1	2,000
Trinitroanisole	606-35-9	2,000
Trinitrobenzene	99-35-4	2,000
Trinitrobenzenesulfonic acid	2508-19-2	2,000
Trinitrobenzoic acid	129-66-8	2,000
Trinitrochlorobenzene	88-88-0	2,000
Trinitrofluorenone	129-79-3	2,000
Trinitro-meta-cresol	602-99-3	2,000
Trinitronaphthalene	558101-17-8	2,000
Trinitrophenetole	4732-14-3	2,000
Trinitrophenol	88-89-1	2,000
Trinitroresorcinol	82-71-3	2,000
Trinitrotoluene	118-96-7	2,000
Tris(2-chloroethyl)amine	555-77-1	Any Amount
Tris(2-chlorovinyl)arsine	40334-70-1	Any Amount
Tritonal	54413-15-9	2,000
Tungsten hexafluoride	7783-82-6	Any Amount
Uranium hexafluoride	7783-81-5	2,000
Urea	57-13-6	2,000
Urea nitrate	124-47-0	2,000
Vinyl acetate monomer	108-05-4	11,250
Vinyl actylene	689-97-4	7,500
Vinyl chloride	75-01-4	7,500
Vinyl ethyl ether	109-92-2	7,500
Vinyl fluoride	75-02-5	7,500
Vinyl methyl ether	107-25-5	7,500
Vinylidene chloride	75-35-4	7,500
Vinylidene fluoride	75-38-7	7,500
Vinyltrichlorosilane	75-94-5	2,000
Zinc dithionite	7779-86-4	2,000
Zinc hydrosulfite	7779-86-4	2,000
Zirconium picramate	63868-82-6	2,000

Date:

Michael Chertoff
Secretary of Homeland Security
Department of Homeland Security