AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

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) of this section 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, the calculation provisions in § 27.203, and the minimum concentration provisions in § 27.204 if it possesses any of the chemicals listed in appendix A to this part at or above the STQ for any applicable Security Issue.

(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 paragraph (c)(1) of this section 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.

[72 FR 17729, Apr. 9, 2007, as amended at 72 FR 65418, Nov. 20, 2007]

§27.203 Calculating the screening threshold quantity by security issue.

(a) *General.* In calculating whether a facility possesses a chemical of interest that meets the STQ for any security issue, a facility need not include chemicals of interest:

(1) Used as a structural component;

(2) Used as products for routine janitorial maintenance;

(3) Contained in food, drugs, cosmetics, or other personal items used by employees;

(4) In process water or non-contact cooling water as drawn from environment or municipal sources;

(5) In air either as compressed air or as part of combustion;

(6) Contained in articles, as defined in 40 CFR 68.3;

(7) In solid waste (including hazardous waste) regulated under the Resource Conservation and Recovery Act, 42 U.S.C. 6901 *et. seq.*, except for the waste described in 40 CFR 261.33;

(8) in naturally occurring hydrocarbon mixtures prior to entry of the mixture into a natural gas processing plant or a petroleum refining process unit. Naturally occurring hydrocarbon mixtures include condensate, crude oil, field gas, and produced water as defined in 40 CFR 68.3.

(b) *Release chemicals*—(1) *Release-toxic, release-flammable, and release-explosive chemicals.* Except as provided in paragraphs (b)(2) and (b)(3), in calculating whether a facility possesses an amount that meets the STQ for release chemicals of interest, the facility shall only include release chemicals of interest:

(i) In a vessel as defined in 40 CFR 68.3, in a underground storage facility, or stored in a magazine as defined in 27 CFR 555.11;

(ii) In transportation containers used for storage not incident to transportation, including transportation containers connected to equipment at a facility for loading or unloading and transportation containers detached from the motive power that delivered the container to the facility;

(iii) Present as process intermediates, by-products, or materials produced incidental to the production of a product if they exist at any given time;

(iv) In natural gas or liquefied natural gas stored in peak shaving facilities; and

(v) In gasoline, diesel, kerosene or jet fuel (including fuels that have flammability hazard ratings of 1, 2, 3, or 4, as determined by using National Fire Protection Association (NFPA) 704: Standard System for the Identification of the Hazards of Materials for Emergency Response [2007 ed.], which is incorporated by reference at 27.204(a)(2)) stored in aboveground tank farms, including tank farms that are part of pipeline systems;

(2) *Release-toxic, release-flammable, and release-explosive chemicals.* Except as provided in paragraph (c)(2)(i), in calculating whether a facility possesses an amount that meets the STQ

for release-toxic, release-flammable, and release-explosive chemicals, a facility need not include release-toxic, release-flammable, or release-explosive chemicals of interest that a facility manufactures, processes or uses in a laboratory at the facility under the supervision of a technically qualified individual as defined in 40 CFR 720.3.

(i) This exemption does not apply to specialty chemical production; manufacture, processing, or use of substances in pilot plant scale operations; or activities, including research and development, involving chemicals of interest conducted outside the laboratory.

(ii) [Reserved]

(3) *Propane.* In calculating whether a facility possesses an amount that meets the STQ for propane, a facility need not include propane in tanks of 10,000 pounds or less.

(c) *Theft and diversion chemicals.* In calculating whether a facility possesses an amount of a theft/diversion chemical of interest that meets the STQ, the facility shall only include theft/diversion chemicals of interest in a transportation packaging, as defined in 49 CFR 171.8. Where a theft/diversion-Chemical Weapons (CW) chemical is designated by ''CUM 100g,'' a facility shall total the quantity of all such designated chemicals in its possession to determine whether the facility possesses theft/diversion-CW chemicals that meet or exceed the STQ of 100 grams.

(d) *Sabotage and contamination chemicals.* A facility meets the STQ for a sabotage/contamination chemical of interest if it ships the chemical and is required to placard the shipment of that chemical pursuant to the provisions of subpart F of 49 CFR part 172.

[72 FR 65419, Nov. 20, 2007]

§ 27.204 Minimum concentration by security issue.

(a) *Release chemicals*—(1) *Release-toxic chemicals.* If a release-toxic chemical of interest is present in a mixture, and the concentration of the chemical is equal to or greater than one percent (1%) by weight, the facility shall count the amount of the chemical of interest in the mixture toward the STQ. If a release-toxic chemical of interest is present in a mixture, and the concentration of the chemical is less than one percent (1%) by weight of the mixture, the facility need not count the amount of that chemical in the mixture in determining whether the facility possesses the STQ. Except for oleum, if the concentration of the chemical of interest in the mixture is one percent (1%) or greater by weight, but the facility can demonstrate that the partial pressure of the regulated substance in the mixture (solution) under handling or storage conditions in any portion of the process is less than 10 millimeters of mercury (mm Hg), the amount of the substance in the mixture in that portion of a vessel need not be considered when determining the STQ. The facility shall document this partial pressure measurement or estimate.

(2) *Release-flammable chemicals.* If a release-flammable chemical of interest is present in a mixture in a concentration equal to or greater than one percent (1%) by weight of the mixture, and the mixture has a National Fire Protection Association (NFPA) flammability hazard rating of 4, the facility shall count the entire amount of the mixture toward the STQ. Except as provided in § 27.203(b)(1)(v) for fuels that are stored in aboveground tank farms (including farms that are part of pipeline systems), if a release-flammable chemical of interest is present in a mixture in a concentration equal to or greater than one percent (1%) by weight of the mixture, and the mixture has a National Fire Protection Association (NFPA) flammability hazard rating of 1, 2, or 3, the facility need not count the mixture toward the STQ. The flammability hazard ratings are defined in NFPA 704: Standard System for the Identification of the Hazards of Materials for Emergency Response [2007 ed.]. The Director of the Federal Register approves the incorporation by reference of this standard in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. You may obtain a copy of the incorporated standard from the National Fire Protection Association at 1 Batterymarch Park, Quincy, MA 02169–

7471 or *http://www.nfpa.org*. You may inspect a copy of the incorporated standard at the Department of Homeland Security, 1621 Kent Street, 9th Floor, Rosslyn VA (please call 703–235–0709) to make an appointment or at the or at the National Archives and Records Administration (NARA). For information on the availability of material at NARA, call 202–741–6030, or go to *http://www.archives.gov/federal__register/code__of__federal__regulations/ibr__locations.html*. If a release-flammable chemical of interest is present in a mixture, and the concentration of the chemical is less than one percent (1%) by weight, the facility need not count the mixture in determining whether the facility possesses the STQ.

(3) *Release-explosive chemicals.* For each release-explosive chemical of interest, a facility shall count the total quantity of all commercial grades of the chemical of interest toward the STQ, unless a specific minimum concentration is assigned in the Minimum Concentration column of appendix A to part 27, in which case the facility should count the total quantity of all commercial grades of the chemical at the specified minimum concentration.

(b) *Theft and diversion chemicals.* (1) Theft/Diversion-Chemical Weapons (CW) and Chemical Weapons Precursors (CWP Chemicals: Where a theft/diversion-CWC/CWP chemical of interest is not designated by ''CUM 100g'' in appendix A, and the chemical is present in a mixture at or above the minimum concentration amount listed in the Minimum Concentration column of appendix A to part 27, the facility shall count the entire amount of the mixture toward the STQ.

(2) Theft/Diversion-Weapon of Mass Effect (WME) Chemicals: If a theft/diversion-WME chemical of interest is present in a mixture at or above the minimum concentration amount listed in the Minimum Concentration column of appendix A to part 27, the facility shall count the entire amount of the mixture toward the STQ.

(3) *Theft/diversion-Explosives/Improvised Explosive Device Precursor (EXP/IEDP) chemicals.* For each theft/diversion-EXP/IEDP chemical of interest, a facility shall count the total quantity of all commercial grades of the chemical toward the STQ, unless a specific minimum concentration is assigned in the Minimum Concentration column of appendix A to part 27, in which case the facility should count the total quantity of all commercial grades of the chemical at the specified minimum concentration.

(c) *Sabotage and contamination chemicals.* For each sabotage/contamination chemical of interest, a facility shall count the total quantity of all commercial grades of the chemical toward the STQ.

[72 FR 65419, Nov. 20, 2007]

§ 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) of this

section 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) Unless otherwise notified, within 60 calendar days of November 20, 2007 for facilities that possess any of the chemicals listed in appendix A at or above the STQ for any applicable Security Issue, or within 60 calendar days for facilities that come into possession of any of the chemicals listed in appendix A at or above the STQ for any applicable Security Issue; 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) of this section, 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) of this section , 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.

[72 FR 17729, Apr. 9, 2007, as amended at 72 FR 65420, Nov. 20, 2007]

§ 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 schedule provided in §27.210.

(2) Notwithstanding paragraph (d)(1) of this section, 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 or 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 system, 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.

(b) [Reserved]

§ 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 Assessment 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) of this section, 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) of this section, 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) of this section and issues an Order Assessing Civil Penalty pursuant to paragraph (b)(1) of this section, 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, if the violation of the Order occurred on or before November 2, 2015, or $32,796 for each day during which the violation of the Order continues, if the violation occurred after November 2, 2015.

(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.

[72 FR 17729, Apr. 9, 2007, as amended at 81 FR 43001, July 1, 2016]

§ 27.305 Neutral adjudications.

(a) Any facility or other person who has received a Finding pursuant to § 27.230(a)(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