Summary of Public Comments Received on the Draft *Risk Based Performance Standards Guidance Document* and the Department of Homeland Security's Response to the Comments

On October 4, 2006, Section 550 of the Department of Homeland Security Appropriations Act of 2007 provided the Department of Homeland Security (DHS or the Department) with the authority to regulate the security of high-risk chemical facilities. See Pub. L. 109-295. Section 550 requires the Secretary of Homeland Security to promulgate interim final regulations "establishing risk-based performance standards for security of chemical facilities." Id.

On April 9, 2007, the Department issued such interim final regulations in a new Part 27 to Title 6 of the Code of Federal Regulations. See 72 FR 17688. These regulations, the Chemical Facility Anti-Terrorism Standards (CFATS), require high-risk chemical facilities to prepare Security Vulnerability Assessments (SVAs) and develop and implement Site Security Plans (SSPs) that address vulnerabilities identified in the SVA and meet the requirements set forth in eighteen risk-based performance standards (RBPSs) established by the CFATS regulations.

To assist high-risk facilities in the selection and implementation of appropriate protective measures and practices to satisfy the eighteen RBPSs, and to assist DHS personnel in evaluating those measures and practices consistently for purposes of CFATS compliance, the Department developed a *Risk-Based Performance Standards Guidance Document* (Guidance). On October 27, 2008, the Department released for public review and comment a draft version of the Guidance that had been developed by the Department in collaboration with Federal, State, local, and private sector security partners. The public comment period for the draft version of the Guidance closed on November 26, 2008. The Department received approximately thirty sets of comments from a variety of private companies, industry organizations, and public interest groups. All of these comments are publicly available online via www.regulations.gov. Based on the comments received during this comment period, the Department has, where appropriate, revised the Guidance. The Department has made the final Guidance available to high-risk chemical facilities via the Chemical Security Assessment Tool web portal for use during the development of the covered facilities' SSPs.

The following is a summary of the comments submitted to the Department, as well as the Department's response to those comments. For convenience, we have divided the comments into two broad categories: (1) general comments and (2) comments focused on a specific security issue or specific RBPS.[1] Within these two categories, we have further broken down the comments into a variety of subcategories. These subcategories are as follows:

[1] Many of the comments incorrectly refer to "requirements" or "recommendations" contained in the draft Guidance. In the following responses to those specific comments, whether or not the responses explicitly say so, DHS disagrees with every commenter that claims or implies the Guidance imposes any requirements at all or even recommends any particular security option over other potential options.

A. General Comments

1. Disclaimers

Comment: Two commenters stated that the disclaimers regarding the proper use of the Guidance are repeated too frequently in the Guidance. Both thought a single disclaimer would suffice. Conversely, one commenter was favorable towards the disclaimers at the beginning of each chapter and three other commenters were favorable towards the disclaimers in general.

Response: To make the Guidance shorter and easier to read, the Department has decided to replace most of the disclaimers and related language with a single disclaimer at the beginning and in a brief footer on every page.

2. Authority over Chemicals other than Chemicals of Interest (COI)

Comment: Five commenters expressed concern that the Guidance either implies or explicitly states that the Department has the authority to regulate chemicals/assets that are not listed as COI in Appendix A to CFATS. Consistent with this, they asserted that DHS

should remove the phrases “hazardous materials” and “dangerous chemicals” from the Guidance and replace them with “COI.”

Response: DHS disagrees with these comments and has not revised the Guidance in this regard. Section 550 of the DHS Appropriations Act of 2007 provides the Department with the authority to regulate the security of high-risk chemical facilities; it does not limit the Department’s authority to specific chemicals. The CFATS regulations were developed in accordance with that authority, and nothing in CFATS – including the RBPSs themselves – limits the scope of the security measures that high-risk facilities must include in their SSPs to COI. The Guidance is consistent with the scope and language of CFATS and the RBPSs. In particular, the phrases in the draft Guidance identified by the commenters as causing concern (i.e., “hazardous materials” and “dangerous chemicals”) are identical to the language used in RBPS 5 (Shipping, Receipt, and Storage) and RBPS 6 (Theft and Diversion). See 6 CFR §§ 27.230(5) and (6).

In using the terms "hazardous materials" in RBPS 5 and “potentially dangerous chemicals" in RBPS 6, DHS generally means COI as listed in Appendix A of CFATS. Those terms may also include, however, other chemicals at a covered facility that pose risks comparable to, or that substantially contribute to, the risks posed by COI listed in Appendix A (i.e., chemicals that have the potential to create significant adverse consequences to human life or health if that facility is subjected to terrorist attack, compromise, infiltration, or exploitation). DHS expects covered facilities to be familiar with their own chemicals (e.g., to know which chemicals are hazardous materials under the Federal hazardous materials transportation laws administered by the U.S. Department of Transportation, 49 U.S.C. §§ 5101, et seq.). Any facility that needs assistance, however, in determining which chemicals and hazardous materials must be addressed under RBPS 5 or 6 in its SSP may request technical assistance from DHS. DHS has inserted a footnote into the Guidance addressing this.

3. Use of the Guidance by Inspectors/Fear of De Facto Standard

Comment: A few commenters expressed concern that DHS Chemical Security Inspectors would use the Guidance or checklists drawn from it as a de facto inspection standard. They asserted this would be a violation of the statutory provision that prevents the Department from approving or disapproving an SSP based on the presence or absence of a particular security measure. The commenters requested the Department explicitly state within the Guidance that the Guidance will not be used as a de facto standard, and to clarify in the Guidance how inspectors will use it.

Response: Inspectors naturally will use the Guidance to help inform the SSP inspection process; however, it will not be used as a de facto checklist. The Guidance already contains sufficient disclaimers explicitly stating that the Guidance does not create any new requirements that a chemical facility must meet beyond what is required by the CFATS regulations themselves. Accordingly, DHS has not revised the Guidance based on these comments.

4. Defining Terminology and Use of Numeric Benchmarks

Comment: Multiple commenters requested that DHS further define or clarify certain terms, including the following: "sufficient delay," "regular interval," "appropriate," "vigorous" v. "extremely vigorous" v. "very likely," and "critical area" v. "secure area" v. "restricted area." Conversely, multiple commenters thought the Department was overly prescriptive in a variety of areas, including, for example, the percent of vehicle inspections in Metric 3.4; the elevated threat response times in Metric 13.2; vehicle barrier requirements of Metric 4.2; time limits for removing access under Metric 8.3.3; times for reporting cyber incidents in Metric 8.5.4; the frequency of cyber audits in Metric 8.9; the training requirements of RBPS 11 (Training); the entirety of RBPS 12 (Personnel Surety); and the recordkeeping requirements of RBPS 18 (Records). Finally, one commenter disagreed with the latter commenters, and recommended that the Guidance should be more prescriptive.

Response: By law, the Department is prohibited from disapproving an SSP based on the presence or absence of a specific security measure or activity. See Section 550(a). In light of this, and the fact that the CFATS-regulated community consists of a diverse spectrum of facilities, the CFATS regulations are intended to provide high-risk facilities the flexibility to design security plans that are tailored to their unique security needs. Nevertheless, each facility's SSP must meet the applicable RBPSs established in 6 CFR § 27.230. The Department developed the Guidance to help facilities consider what security measures and activities to include in their SSPs. In designing the Guidance, the Department struck a balance between providing enough detail for the Guidance to be useful without making it seem prescriptive.

Based on the comments received, the Department decided that it would be beneficial to the regulated community to define or clarify a few terms (e.g., "asset," "restricted area") that are important to understanding the RBPSs and/or how they relate to the SSP process. DHS has added those terms to the final version of the Guidance.

The Department also agrees with the commenters that numerical benchmarks may be mistakenly perceived by some readers as prescriptive and has removed all numeric benchmarks from the metrics with the exception of those benchmarks specifically contained in the regulations (e.g., the length of time records must be kept). The Department believes that the final version of the Guidance strikes an appropriate balance between providing useful guidance and maintaining compliance flexibility.

5. Applicability of the Guidance to Chemical Facilities that are not Large Industrial Sites

Comment: A few commenters noted that the Guidance appears to be written primarily for large, industrial chemical manufacturers, and that many of the recommendations and metrics contained therein may not apply at other types of regulated facilities (e.g.,

unmanned facilities; smaller, urban facilities; gasoline storage facilities which are visited by hundreds of trucks per day). They suggested the Department should make sure that the Guidance addresses the unique characteristics, needs, and conditions of the many different types of regulated facilities.

Response: The Department is aware that the regulated community is composed of a variety of different types of facilities and that a security approach that is appropriate for one facility is not necessarily appropriate for all types of facilities. The Guidance explicitly acknowledges that specific measures contained in the Guidance that may be appropriate for some of the more traditional segments of the regulated community (e.g., chemical manufacturers, oil refineries) may not be appropriate or necessary for other types of regulated facilities (e.g., universities, hospitals, agricultural facilities). The Department invites all regulated facilities to consider the Guidance to the extent applicable to their unique characteristics, and is committed to cooperating with the regulated community to identify and develop appropriate security measures that will satisfy the RBPSs under the circumstances applicable to various types of facilities. Over time, the Department may consider drafting guidance materials tailored to individual segments of the regulated community.

Comment: One commenter noted that the Guidance fails to provide guidance on how to develop an Alternative Security Program (ASP) for colleges and universities.

Response: As previously stated, DHS currently is not developing tailored guidance for each industry segment with facilities subject to CFATS. Additionally, instructions on how to develop an ASP would not be an appropriate topic for inclusion in the Guidance. Accordingly, DHS did not modify the Guidance based on this comment.

6. Asset-Specific v. Facility-Wide Security Measures

Comment: Multiple commenters indicated support for the principle that asset-specific measures can be used in place of facility-wide measures where appropriate. One commenter requested that DHS more clearly state this in RBPS 1 (Restrict Area Perimeter). Two commenters noted that footnote 10 seems to contradict this by saying that certain measures need to be employed “at the macro level.” They recommended deleting or clarifying that footnote.

Response: Although certain RBPS are intended to be applied facility-wide, the Department agrees that, in many circumstances, asset-specific security measures may be cost-effective alternatives to facility-wide measures, and facilities have the flexibility to consider using asset-specific measures in place of or in addition to facility-wide measures where appropriate. The Guidance already clearly states this in RBPS 1, and thus DHS did not modify the Guidance based on those comments. The Department does, however, agree that a reader might misconstrue the reference in footnote 10 to “macro level” security, and so the Department has deleted that reference from the footnote.

7. Harmonization with other Regulations

Comment: Multiple commenters asserted that the Department should try to harmonize CFATS with other Federal regulations wherever possible, and that the Guidance should address the areas of overlap with other regulations. Two commenters also asserted that the Guidance should state that measures that conform to regulations, standards, protocols, or guidelines issued or approved by other Federal agencies will satisfy the applicable RBPS standard.

Response The comments on harmonizing CFATS with other federal programs are beyond the scope of the draft Guidance and require no response. The Department does not agree with the comments that a measure or activity that is compliant with another federal program should automatically be considered to satisfy any RBPS under CFATS. The Department did not change the Guidance based on those comments.

8. Timing of Release of the Guidance

Comment: A few commenters stressed that the Department should not delay in releasing the Guidance, because CFATS facilities are subject to strict compliance dates. The commenters assert that any delay in releasing the guidance could present a compliance problem for some facilities.

Response: The Department agrees that undue delay in the release of the Guidance would make compliance more difficult for covered facilities required to submit SSPs. Thus, DHS released the final Guidance concurrently with final notification of Tier 1 facilities that they are required to submit SSPs within 120 days of that notification.

B. Comments on Specific Security Issues or Risk-Based Performance Standards

1. Security Force/Armed Guards/Interdiction

Comment: Six commenters objected to the inclusion of interdiction as a goal in Metric 4.5. These commenters perceived that Metric 4.5 implicitly requires facilities to employ armed guards and objected to such a requirement. They argued that interdiction is an inappropriate goal for a chemical facility and should be left to local law enforcement (LLE), and that armed guards present a safety concern and cause increased liability and other costs.

One commenter went further and stated that no guards, armed or unarmed, should be required. This commenter asserted that detection systems combined with LLE response should be considered sufficient at certain facilities, such as industrial gas facilities. A different commenter disagreed, asserting that security personnel are crucial to good

security and are an appropriate part of a high-risk chemical facility's security posture. One commenter wanted to know how the interdiction requirement will be applied to unmanned sites.

Response: Contrary to the assertions made by the commenters, Metric 4.5 does not require facilities to hire armed guards, nor does it require interdiction. As previously noted, all of the metrics in the Guidance are merely targets for facilities to consider achieving rather than requirements; nothing, including armed guards or interdiction, is required by the metrics. Moreover, to the extent that Metric 4.5 provides a target that facilities may consider trying to achieve, the metric simply refers to a facility's ability to detect and initiate a response to armed intruders that results in their interdiction. While an armed security force is one potential way of accomplishing this (and something high-risk chemical facilities may wish to consider), there are many other options for achieving this result (e.g., establishing capabilities to detect an attack early enough and delay it long enough so that local law enforcement can intervene; implementing process controls or systems that rapidly render a target non-hazardous even if an attack successfully breaches containment). DHS does not believe it is necessary to revise the discussion in the Guidance regarding Metric 4.5.

Comment: One commenter wanted more detailed descriptions of what type of security forces are appropriate for different facilities/situations.

Response: The Guidance already acknowledges that an appropriate security force depends on a wide variety of factors including, but not limited to, the size of the facility, the physical characteristics of the facility, the risk-level of the facility, the chemicals onsite at the facility, other security measures in place at the facility, and the location and response time of local law enforcement. A facility has broad latitude to decide what type of security force is appropriate for the facility, and the Guidance does not need to provide detailed descriptions. Accordingly, the Department did not change the Guidance based on this comment.

2. Personnel Surety

Comment: One commenter stated that the Guidance expands the scope of background checks beyond the regulations and that the guidance on background checks is overly prescriptive.

Response: DHS disagrees. The Guidance is consistent with the language of RBPS 12 (Personnel Surety) in the CFATS regulation, 6 CFR § 27.230(a)(12). In the final Guidance, however, DHS has further clarified that, as provided in CFATS, background checks are required only for facility personnel and unescorted visitors with access to restricted areas or critical assets at high-risk facilities.

Comment: One commenter stated that the regulations and the Guidance fail to protect employees from excessive background checks.

Response: Protecting individual citizens from what an employee may consider to be excessive background checks is not within the scope of CFATS or the Guidance. Accordingly, DHS did not modify the Guidance based on this comment. Privacy, employment, and labor laws, however, may protect chemical facility employees from "excessive" background checks.

Comment: The Department received multiple comments on the redress discussion contained in the chapter of the Guidance on RBPS 12 (Personnel Surety). Three commenters noted that a redress/appeals process is corporate-wide, not facility specific, and thus any requirements regarding a redress/appeals process under CFATS likely would have impacts on a company beyond its regulated facilities. Two of those commenters recommended that DHS not provide any guidance on this matter other than suggesting that a facility have a redress process. The third commenter asserted that even that was too much, arguing that DHS should delete the redress requirement in its entirety as it is an attempt by the Department to impose administrative proceedings on CFATS facilities that have nothing to do with the protection and safeguarding of the facilities. Another commenter suggested that DHS should eliminate the redress process discussion for a different reason – because facilities are ill-equipped to manage such a program, especially in light of the regulation's requirement to check individuals for terrorist ties.

Two commenters suggested removing the example adjudication process from Appendix C, arguing that companies should decide on the process based upon company criteria and labor law.

Response: Upon reviewing the comments, the Department understands how a facility might construe the redress process described in the draft Guidance as going beyond the requirements of RBPS 12. Further, the Department realizes that this area is the subject of well-established employment law. Thus, the Department has decided to remove all discussion of company redress processes from both the Guidance's chapter on RBPS 12 (Personnel Surety) and from Appendix C of the Guidance.

Comment: One commenter sought clarification on whether or not a redress/appeals process was necessary at the facility level for an adverse Terrorist Screening Database (TSDB) finding. The same commenter asked whether or not an applicant who receives an adverse TSDB finding can or must involve his/her facility in the administrative appeals process.

Response: For the reasons stated in response to the previous comment, the Department has decided to remove all discussion of company redress processes from the discussion of RBPS 12. Challenges to any finding under RBPS 12 that a person has terrorist ties and is a potential security threat may be made through the adjudication and appeals proceedings

established by CFATS. See 6 CFR §§ 27.305 – 27.345. Whether or not an individual involves the facility in such a redress proceeding would typically depend on the specific circumstances.

Comment: The Department received multiple comments concerning the use of Transportation Worker Identification Credential (TWIC) cards in regard to the CFATS Personnel Surety effort. One commenter stated that the Guidance should clarify whether possession of a TWIC card will satisfy RBPS 12 requirements and whether or not TWIC holders still must go through the TSDB check. Two commenters asserted that a TWIC card should satisfy the CFATS personnel surety requirements while one commenter disagreed with them.

Response: In the preamble to the CFATS regulation the Department stated that "[t]o 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, a hazardous materials endorsement (HME) license, a NEXUS credential, or a Free and Secure Trade (FAST) credential, will not need to undergo additional vetting by DHS." 72 FR 17709 (April 9, 2007). DHS has added a statement to that effect to the Guidance. Additionally, DHS has added a section to the Guidance making it clear that an individual who possesses a current, authentic TWIC meets the background check requirements in 6 CFR § 27.230(12)(i)-(iv).

Comment: Two commenters noted that there are good opportunities for harmonization with other Federal regulations when it comes to RBPS 12 (Personnel Surety), in particular with the Federal government's rail security efforts.

Response: The comments on harmonizing CFATS with other federal programs are beyond the scope of the draft Guidance and require no response. In the future, as DHS continues to implement CFATS, we will continue to look for and pursue opportunities to harmonize this regulation with other Federal regulations.

Comment: One commenter stated that DHS should make it explicit that a chemical facility that is a Maritime Transportation Security Act (MTSA) facility must comply with the RBPS 12 (Personnel Surety) requirements, because all chemical facilities should be regulated as chemical facilities under CFATS.

Response: The authorizing statute, at Section 550(a), provides that CFATS shall not apply to facilities regulated under MTSA. This exemption cannot be modified or revoked by DHS either in CFATS or in the Guidance.

Comment: One commenter requested that DHS explicitly state that third-parties may manage the personnel surety program for regulated facilities. Another commenter asked

if third party providers will be able to play a role in the TSDB process (i.e., can they submit employee information on behalf of a facility).

Response: DHS has revised the final Guidance to clarify that a facility may hire a third-party to help manage the facility's personnel surety program. As for third-party involvement in the TSDB process, the Department is still determining the mechanism through which facilities will satisfy 6 CFR §27.230(12)(iv), and so cannot state with certainty if there will be a role for third-party providers in that process.

Comment: One commenter requested that the Guidance state that facilities will be given wide discretion to determine how best to handle an employee who receives a positive hit during a background check.

Response: Appendix C of the Guidance discusses background checks and their associated procedures, including the fact that final determinations on employment actions are the responsibility of the facility. As stated in the Guidance, DHS expects that chemical facilities will use data generated as part of CFATS-required background checks for lawful purposes only, and will observe all applicable local, state, and Federal labor, employment, and privacy laws in using and handling data acquired as part of background checks. DHS did not revise the Guidance based on this comment.

Comment: One commenter indicated that the Guidance is neither clear as to what types of criminal history checks are appropriate for each tier nor states when a national criminal scan is appropriate. Another commenter claimed that criminal check databases typically are not available to private citizens and thus the discussion of them should be deleted.

Response: The Department believes that it has provided the appropriate level of guidance on background checks and that providing additional guidance on what type of criminal history checks should be applied to each tier could be perceived as prescriptive. Accordingly, the Department has not modified the Guidance based on this comment. In regard to the claim that criminal check databases are not available to the public, the Department disagrees. Most state and county governments allow criminal records searches by employers, and, if a company does not want to contact each applicable jurisdiction individually, there are numerous commercial services that will perform nationwide criminal records searches for a fee.

Comment: One commenter asked for clarification on how frequently covered facilities should perform personnel surety audits for Tier 1 and 2 facilities. The same commenter stated that the Guidance and regulations are contradictory because the regulations require facilities to audit their SSPs annually, while the Guidance says Tier 3 and 4 facilities do not need to conduct audits of their personnel surety programs.

Response: The commenter is correct that, pursuant to 6 CFR § 27.225(e), a covered facility must conduct an annual audit of its compliance with its SSP. As part of this annual compliance audit, a facility should audit its personnel surety program, which is part of the facility's SSP. DHS has changed Metric 12.4 to acknowledge that each facility, regardless of tier, must audit its personnel surety program annually.

Comment: One commenter suggested that the Guidance should affirmatively state that CFATS does not shield facilities from liability if they violate Federal or state law when performing background checks. Conversely, one commenter suggested the Guidance should state that DHS approval of an SSP authorizes a facility to state that its relevant employment practices are required by the RBPSs and approved by DHS.

Response: Approval of an SSP merely reflects the Department's determination that the SSP satisfies the applicable RBPSs under CFATS. It is not an implicit or explicit statement on the compliance of the facility's personnel surety program with Federal, state, or local employment, labor, or privacy laws. It is the facility's responsibility to ensure that those laws are being met, and CFATS does not automatically shield covered facilities from liability if their personnel surety programs violate other Federal, state, or local law. If a facility believes, however, that a state or local law is in direct conflict with CFATS, and thus preempted, the facility may seek an opinion from DHS under 6 CFR § 27.405.

Comment: One commenter asked whether a facility can use the results of a background check that a previous employer has performed on an employee.

Response: Whether or not a facility can use the results of a background check that a previous employer performed on an employee is dependent on the specific circumstances. The Department will determine the acceptability of this approach during a review of the facility's SSP. Thus, no change to the Guidance is required.

Comment: One commenter stated that it is illogical (and potentially contradictory with Metric 6.3) for Metric 12.3 to make background checks of contractors prior to access optional while background checks for employees prior to access are mandatory. The commenter recommends that DHS change the metric to require background checks on contractors.

Response: The Department agrees that there should be no distinction between employees and contractors when determining whether the facility should perform a background check. Under RBPS 12, background checks are required for facility "personnel" and unescorted visitors with access to restricted areas or critical assets, and does not depend on whether the "personnel" are employees or contractors. This principle is captured in the RBPS 12 summary in Table 17, as well as in Metric 12.1. DHS has

amended Metric 12.2, however, to discuss background checks on existing contractors, and has deleted the potentially inconsistent language in Metric 12.3.

Comment: One commenter stated that it is unclear how a facility is supposed to verify the background of every United Parcel Service and Federal Express delivery truck driver with which it does business, and thinks the requirement of background checks on contractors or visitors is overly burdensome. This commenter recommended that DHS apply the background check requirements for contractors or visitors (e.g., third-party drivers) only for shipments exceeding the screening threshold level of COI or, preferably, only to Tier 1 and Tier 2 facilities.

Response: DHS does not agree that any revision to the Guidance is warranted in regard to this comment. Consistent with RBPS 12, the Guidance addresses background checks for visitors given *unescorted access to restricted areas*. RBPS 12 does not require, and the Guidance does not suggest, that the facility pre-screen every third-party visitor to the site prior to entry. Moreover, as mentioned repeatedly throughout the Guidance, the security alternatives presented in the Guidance are simply alternative options for consideration. None of the measures, activities, or metrics contained in the Guidance are requirements.

Comment: One commenter asserted that requiring all employees at a facility whose sole security issue is theft/diversion to undergo background checks is unnecessary. The commenter suggested that DHS should limit the requirement to those employees given access to COI in storage, not those who merely deal with the COI at some point during the manufacturing process.

Response: DHS disagrees with this comment, and thus has not changed the Guidance in response to it. RBPS 12 requires background checks for all personnel and unescorted visitors with access to any restricted area or critical asset at a facility. The final Guidance makes clear that a COI may be a critical asset, and since a COI could be stolen from a manufacturing process as well as from a storage location by an unauthorized person with access to it, background checks should not be limited to those persons who have access to a theft/diversion COI in a storage location (e.g., a warehouse).

Comment: One commenter asserted that employment history background checks and Department of Motor Vehicles (DMV) checks are not appropriate as they concern a person’s qualifications to perform a job, not his/her suitability to work in a secure environment.

Response: DHS disagrees. Although the security measures identified in the Guidance are simply options for consideration and not requirements, the Department believes that both employment history and DMV checks can be useful for verifying a person’s

suitability to work in a secure environment since both procedures can uncover potential inconsistencies or discrepancies that could lead to the identification of security issues.

Comment: One commenter noted that the draft Guidance states that existing employees are not allowed access to restricted areas until a background check is completed, which may require companies to shut down facilities until those checks are completed. The commenter asserted that this is unreasonable, especially considering that companies have previously vetted existing employees through the hiring process. This commenter recommended that DHS remove this requirement.

Response: DHS reiterates that the Guidance itself does not impose any requirements on facilities or employees. The Department agrees, however, that the draft Guidance could have been misconstrued as suggesting that facilities consider prohibiting existing employees from accessing restricted areas until after a background check has been completed. Consistent with the discussion of RBPS 12 in the preamble to the CFATS Interim Final Rule, facilities should submit with their SSPs the names of individuals needing background checks, and should proceed with the background checks once DHS issues the facility a Letter of Authorization preliminarily approving the facility's SSP. See 72 Fed. Reg. 17708. Under that approach, by the time an SSP is fully approved, there should not be any significant interruption in work as a result of the need to perform background checks. The Department, however, has deleted from Metric 12.2 the statement regarding not providing access to restricted areas until after a background check is complete.

Comment: One commenter stated that security personnel should be subject to a personnel surety program.

Response: While the Department agrees that security personnel, whether employees or contractors, with access to restricted areas or critical assets should be subject to the personnel surety program, the Guidance adequately addresses that fact. DHS does not believe that any further revision is warranted.

3. Training

Comment: Two commenters noted that the training requirements in Table 14 and those in the text are inconsistent. One commenter asserted that the training requirements are prescriptive.

Response: DHS has modified the Guidance to eliminate any potential inconsistencies between Table 14 and other text on training, as well as any training-related material that may have given the appearance of prescriptiveness.

Comment: Two commenters recommended that the requirement to conduct exercises be eliminated.

Response: The Guidance does not contain any requirement that regulated facilities conduct exercises. The Guidance on exercises merely suggests that regulated facilities consider exercises, among other security alternatives, in addressing RBPS 11 (Training). Accordingly, DHS did not modify the Guidance based on these comments.

Comment: One commenter requested that DHS include more detailed guidance (than what is in Table 13) on recommended training.

Response: The Department believes that the Guidance currently possesses the appropriate level of detail. DHS does not believe that any change to the Guidance is necessary in response to this comment.

Comment: One commenter stated that the training requirements are not applicable as written to the industrial gas industry, where security is managed at a corporate, not site, level.

Response: The Department disagrees. As already stated in the Guidance, the Department recognizes that for many companies with multiple facilities, security will be managed at the corporate level. Nevertheless, simply because security is managed offsite does not mean that facility-level drills, exercises, etc. are inappropriate. Accordingly, DHS did not modify the Guidance based on these comments.

Comment: One commenter stated that the Guidance should provide more detail on sharing Chemical-terrorism Vulnerability Information (CVI) with local agencies in the course of training exercises.

Response: Detailed information regarding the sharing of CVI is contained in the CVI Procedural Manual ("Safeguarding Information Designated as Chemical-terrorism Vulnerability Information," Sept. 2008) available at www.dhs.gov/chemicalsecurity), and no additional detail on this issue is necessary for the Guidance.

4. Emergency Response v. Security Response

Comment: Three commenters indicated that emergency response and security response get confused at times in the Guidance and that the Guidance needs to be reviewed to make sure that the confusion is eliminated.

Response: The Guidance has been reviewed to ensure that there is no confusion between emergency response and security response, and the Department has determined that there is no need to revise the Guidance in this regard.

Comment: One commenter asserted that security personnel likely will have to play an expansive role in any emergency response (e.g., immediately manage the aftermath of an event; properly direct emergency personnel) and that the Guidance should specifically account for this role.

Response: The Department agrees that security personnel may have to play a role in emergency response and has added a sentence to the discussion of RBPS 9 (Response) in the final Guidance acknowledging this.

Comment: One commenter recommended that DHS should separate security response from crisis management.

Response: The Department disagrees. The Guidance expresses no position on whether a facility should integrate security response and crisis management or should keep the activities separate, since it is up to the facility to choose if it wants to handle those issues together or separately.

5. Cybersecurity

Comment: Two commenters commented on the definition of critical cyber assets. One thought the list of potentially critical cyber systems was overly expansive, was broader than that which is considered in the Chemical Security Assessment Tool (CSAT) SVA tool, and asserted that DHS should rewrite it to limit criticality to cyber systems capable of causing a release or realistically contributing to the theft/diversion of a COI. Conversely, the other commenter stated that non-critical systems connected to critical systems may themselves become critical.

Response: Which cyber systems are critical will vary based on the specifics of the facility, such as the materials possessed onsite, the interconnectivity between the facility's cyber systems, and a host of other factors. Accordingly, rather than specifically defining what a critical cyber system is, the Guidance provides a general description of what may make a cyber system critical, and a list of examples of types of cyber systems that may be critical. No further clarification is warranted.

Comment: One commenter requested that DHS define the term "IT," and asserted that the Guidance needs to differentiate between IT systems and control systems and better address control systems.

Response: The Department does not agree that it is necessary to define the term IT for purposes of the Guidance. In regard to control systems, the Guidance already adequately addresses control systems and their potentially unique cybersecurity considerations. Accordingly, DHS did not modify the Guidance based on this comment.

Comment: One commenter thought the organization of the cyber chapter was unclear and concepts were intermixed. This commenter recommended examining the organizational structure of other cybersecurity guidance documents such as the International Society of Automation (ISA) 99 Parts 1 & 2 and the National Institute of Standards and Technology (NIST) 800-53 and 800-82, and including references to those documents.

Response: The Department believes that the organization of the cyber chapter is clear and appropriate; however, the Department has made some slight adjustments to the cyber chapter in response to this comment. The Department also has added the cyber documents recommended by the commenter to the list of additional available resources provided in Appendix C.

Comment: One commenter suggested that DHS add the following specific guidelines to the Guidance: (a) production systems should be tested before implementation; and (b) control system policies and procedures should be specified. Additionally, the commenter suggested the Guidance should provide a warning about "scanning," which the commenter believed may shut down operations just like a virus update.

Response: System testing already is addressed in the Guidance discussion on change management, and a statement regarding the fact that a facility may wish to consider developing policies and procedures specific to control systems has been added to Appendix C of the Guidance. It is unclear what type of scanning the commenter was referring to, and thus no change to the Guidance was made based on that comment.

Comment: One commenter suggested that the Guidance should use the term "safety instrumented system" instead of "watch dog system."

Response: Safety instrumented systems (SIS) are a type of "watch dog system," and are cited in both the draft and final Guidance as such. The Department intentionally used the broader "watch dog" term since facilities may use systems other than SIS as watch dog systems. Given the wide-spread use of SIS, the draft Guidance already contained a section discussing the use of SIS as part of a comprehensive cybersecurity posture. Accordingly, the Department did not modify the Guidance based on this comment.

Comment: One commenter recommended that the Guidance use the definition of "systems boundary" from NIST SP 800-82 because allowing facilities to determine their own boundaries makes determining compliance impossible.

Response: As explained above, the Department has intentionally chosen to leave many terms undefined to provide facilities with maximum flexibility in complying with the RBPS. Thus, DHS has not revised the Guidance as requested by the commenter.

Comment: One commenter claimed that verifying external connections through the use of network tools may not apply to modems and other types of control system connections, and recommended that the "external connections" paragraph be reworded.

Response: The Department believes that, in many cases, the verification of external communications through the use of network tools may apply to modems and other types of control system connections, and thus has not reworded the section of the Guidance discussing external communications.

Comment: One commenter recommended changing the phrase "business purposes" to "safety purposes" in regard to the guidance on unique accounts.

Response: The Department has determined that the term "business purposes" was extraneous in that sentence and has removed it.

Comment: One commenter noted that for control systems, automatic installation of software could be dangerous, and suggested removal of the recommendation that antivirus software get updated automatically. Moreover, the commenter asserted that software or patches should not be added unless they are first checked to ensure that they do no conflict with control software.

Response: Upon further consideration, the Department has revised this portion of the Guidance, indicating that software installation should only occur after appropriate testing. In any event, as is true for the Guidance as a whole, the cybersecurity reference at issue here is merely one of many possible alternatives for consideration by covered facilities; it is not a requirement.

Comment: One commenter noted that the draft Guidance's suggestion that facilities consider filtering e-mail attachments should be modified to state that control systems should not be connected to the internet or be able to receive e-mail.

Response: DHS does not agree that such a modification is necessary. While isolating control systems from the internet and/or e-mail may be appropriate in many cases, there may be instances in which a facility may justifiably have a control system connected to the internet or an e-mail server and still have an appropriate cybersecurity posture.

Comment: One commenter noted that Safety Instrumented Systems take action when something goes wrong anywhere in the system, not just in the cyber system. This commenter also noted that intrusion detection systems (IDS) do not take action, as that would be intrusion response, and that most industrial control systems have intrusion detection, but not intrusion response.

Response: The Department has revised the final Guidance to acknowledge that SIS take action when something goes wrong in the process unrelated to the cyber system as well as when something goes wrong in the cyber system. DHS did not revise the portion of the Guidance discussing IDS, since IDS will take action in response to an intrusion, even if that action is simply to log the intrusion or notify a system monitor.

Comment: One commenter noted that there were two metrics numbered 8.3.1, and, for consistency purposes, suggested adding ".1" to metrics 8.6, 8.7, and 8.9.

Response: The Department has corrected the numbering of the metrics.

Comment: One commenter asserted that Metric 8.5.1 did not sufficiently recommend security controls, that implementing good security controls is fundamental to making improvements to the security posture of the facility, and that the brevity of the statement on security controls could lead one to think that these are not important.

Response: The Department agrees that implementing good security controls is fundamental to a strong security posture; however, the Department believes that Metric 8.5.1 conveys this fact and thus is sufficient as written.

Comment: One commenter recommended that DHS should remove the word "administrative" from Metric 8.3.1.

Response: The Department agrees and has deleted the word "administrative" from Metric 8.3.1.

Comment: One commenter recommended that critical assets should reside within an electronic security perimeter (ESP) with access points that are identified and protected and that a vulnerability assessment of these access points should be conducted at least once annually. The same commenter also recommended using layered security for cyber assets, including an active ESP, a Network Intrusion Detection Systems, a Security Event Manager, and 24x7x365 monitoring.

Response: Security measures similar to those described by this commenter already were discussed in the draft cybersecurity chapter. Accordingly, the Department did not modify the Guidance based on this comment.

Comment: One commenter requested that DHS clarify Metric 8.1.1 (documented and distributed cyber policies) and that Metric 8.1.2 state that the individual responsible for cybersecurity need not be located at the facility.

Response: The Department has already provided sufficient information on cyber policies in the chapter discussing RBPS 8 (Cyber) and no change to Metric 8.1.1 is warranted. In regard to the individual responsible for cyber security, the Department had previously indicated in the chapter discussing RBPS 8 and in the chapter on RBPS 17 (Officials and Organization) that a facility's security official(s) does not need to be located at the facility. The Department believes this does not need to be explicitly stated in Metric 8.1.2.

Comment: One commenter noted that Metric 8.5.4 - Reporting of Cyber Incidents – should make clear how such reports should be made and explicitly state whether or not the reports will be protected as CVI.

Response: DHS has incorporated into the chapter on RBPS 8 (Cyber) additional information regarding the reporting of cybersecurity incidents, including whether or not cybersecurity incident reports will be treated as CVI.

6. Recordkeeping

Comment: Three commenters thought the Guidance should be more specific and provide more meaningful details on the recordkeeping requirements.

Response: The Department believes that the chapter on RBPS 18 (Records) in the draft Guidance, presented the appropriate level of detail. In light of the subjective nature of the appropriate level of detail for material such as this and the Department's belief that the current level of detail is appropriate, the Department did not modify the Guidance based on these comments.

Comment: Two commenters thought the regulatory requirements, such as the requirement to maintain all security awareness training records as CVI, are overly broad and unduly burdensome.

Response: This comment is beyond of the scope of the Guidance because it relates to the CFATS interim final rule. No response is required.

Comment: One commenter asserted that providing lengths of time for which records need to be kept is inappropriately prescriptive.

Response: This comment is beyond the scope of this Guidance since the time periods for keeping records are prescribed by the CFATS regulations, 6 CFR § 27.255, not by the Guidance.

Comment: One commenter requested that the Guidance state that facilities can store records centrally at a company's headquarters instead of onsite.

Response: DHS already states this in the Guidance. No change is necessary.

Comment: One commenter thought DHS should modify Metric 18.2 to make sure it is talking about "security" training records (not all training). The commenter also thought that DHS should require both the retention of investigative reports from incidents and the retention of records of corrective actions taken in Metrics 18.3 and 18.6, respectively.

Response: The Department agrees that the regulatory requirement to maintain records on training, 6 CFR § 27.255(a)(1), was intended to be limited to security-related training. DHS has added a footnote to the chapter of the Guidance discussing RBPS 11 (Training) to clarify this point. As for the additional recordkeeping requirements suggested by the commenter, the CFATS regulation defines the recordkeeping requirements, and the Department cannot add new recordkeeping requirements via the Guidance.

7. Elevated Threats

Comment: One commenter stated that DHS should not mandate specific response timeframes, but should say that response needs to be within a reasonable timeframe.

Response: The Department has removed the suggested time frames associated with response to elevated threats from the Guidance.

Comment: One commenter requested that DHS should allow facilities to use a company-specific threat level system that differs from the DHS Homeland Security Advisory System (HSAS) Threat Level.

Response: While a facility is free to use an additional, company-specific threat level system, DHS believes it is appropriate for the Guidance on RBPS 13 (Elevated Threats) to refer to facilities' plans to respond to changes in the Department's HSAS Threat Level. Thus, no change to the Guidance is necessary.

Comment: One commenter stated that DHS needs to better differentiate between RBPS 13 (Elevated Threats) and RBPS 14 (Specific Threats, Vulnerabilities, or Risks).

Response: RBPS 13 relates to changes in threat levels (e.g., the HSAS Threat Level) which typically address threats to a specific industry (e.g., the Aviation industry) or geographic location (e.g., New York City). RBPS 14, however, relates to threats that are specific to an individual facility. The Department believes that the two are distinct and that they are sufficiently differentiated in the Guidance. The Department did not revise the Guidance based on this comment.

8. Applicability of Specific Security Measures to Gasoline Storage Facilities

Comment: One commenter claimed that issuing badges to all drivers and/or monitoring all individuals without permanent badges as required by Metric 3.2 is impractical for gasoline storage facilities due to the high number of vehicles passing through each day. The commenter also noted that these drivers generally already have TWIC cards, and thus requiring an additional layer of security is unnecessary. Similarly, commenters claimed that the level of vehicle screening required by Metric 3.4 is overly burdensome for gasoline facilities which have large numbers of trucks coming and going every day and that Metric 4.3's requirement of 24/7 security guards or monitored Closed Circuit Television (CCTV) is a waste of resources for gasoline storage facilities.

Response: None of the security measures or activities contained in the Guidance are "required." Nevertheless, in the Guidance, the Department identifies security practices a facility may want to consider. Among those practices the Department believes a Tier 1 or Tier 2 facility should consider, regardless of facility type, is the use of facility-specific ID badges for all individuals. As stated earlier, however, any person possessing a valid TWIC will not need to undergo further background checks under RBPS 12.

In regard to vehicle screening, the Department has removed the reference to a set percentage of vehicles to be inspected from Metric 3.4 in the final Guidance; it is up to the facility to identify and propose an appropriate process for screening incoming vehicles commensurate with the facility's risk level and its unique characteristics.

In regard to the statement regarding Metric 4.3, that metric imposes no such requirements.

Comment: One commenter asserted that Metric 6.7, which recommends vehicle inspections upon egress, is not appropriate for gas terminals as the vehicles that are entering and exiting those facilities simply are tanker trucks delivering gas. The commenter recommended modifying Metric 6.7 to start with the phrase "Where warranted…."

Response: Metric 6.7 is only relevant to a facility that has chemicals for which theft or diversion is a security issue, in which case it is appropriate for such facilities to consider whether to perform vehicle inspections upon egress to ensure theft hazards are not being improperly removed. If a facility, such as a gas terminal, only has release hazards (and thus no theft or diversion hazards), then this metric is irrelevant. Thus, no change to this part of the Guidance is warranted.

9. Miscellaneous Comments

Comment: One commenter suggested the Guidance should discuss the possibility of joint security details among co-located facilities or facilities that share common infrastructure.

Response: DHS agrees that, depending on the circumstances, joint security details among co-located facilities or facilities sharing common infrastructure may be appropriate. DHS has added a sentence acknowledging this as an option in Appendix C.

Comment: One commenter requested that DHS provide additional guidance on the appropriate breadth and scope of visitor controls, stating that it is unclear how visitor control requirements should vary for different tiers and/or categories of facility visitors.

Response: The Department believes that the current guidance on visitor controls (see, e.g., the chapter on RBPS 3; Appendix C) provides sufficient clarity on the subject of visitor controls. Accordingly, DHS did not modify the Guidance based on this comment.

Comment: One commenter stated that Figure 1 on barriers/detection performance does not provide meaningful assistance as it does not differentiate between tiers, does not explain the significance of the times on the x-axis, and is subject to more than one objective interpretation.

Response: Figure 1 is simply meant to demonstrate the benefit that can be gained by detection at the outer perimeter versus detection at an internal asset. That principle does not differ between tiers and does not depend on the hypothetical times on the x-axis of this merely illustrative figure. DHS did not modify the Guidance based on this comment.

Comment: One commenter noted that while the Guidance suggests that safety and security control systems might be merged and housed in a command and control center, this often is not possible.

Response: The Guidance is clear that the merger of these two activities into a single center is only an option that a regulated facility may wish to consider; it is not a

requirement. Whether or not the facility determines such a merger to be practical is up to the facility. DHS did not modify the Guidance based on this comment.

Comment: One commenter noted that, under the non-prescriptive approach being employed by DHS, there is a potential for disagreement between DHS and a facility as to what constitutes an acceptable risk reduction measure. Accordingly, the commenter believed the Guidance should include a chapter describing the process to resolve disagreements that may arise (e.g., appeal procedures).

Response: The CFATS regulations provide procedures for resolving any disputes as to disapproval by DHS of an SSP, including issues related to satisfying any RBPS. See 6 CFR §§ 27.245, 27.305 – 27.345. It is not necessary to add any discussion of those procedures in the Guidance.

Comment: One commenter requested that the Department list approved Alternative Security Programs (ASPs) for Tier 4 facilities in the Guidance, including Sandia's Risk Assessment Methodology for Chemical Facilities (RAM-CF).

Response: This comment is beyond the scope of the Guidance, since ASPs are an alternative to SSPs under the CFATS regulations, but must still satisfy the same RBPSs. In any case, since ASPs are approved on a facility-by-facility basis, it would be premature and inappropriate to list "approved" methodologies in the Guidance.

Comment: Two commenters noted that while the Guidance correctly indicates that many of the performance standards do not apply to facilities where the only security concern is theft or diversion, whether or not an individual performance standard or metric applies is not clear. To help clarify this, the commenters suggested DHS should note that when evaluating how a chemical facility implements the RBPSs, the Department will consider not only the facility's risk tier, but also the nature of the threat involved. Additionally, they recommended that DHS identify within individual metrics if the metric solely applies to facilities with release hazards, and not to facilities that have only theft/diversion hazards.

Response: The Department agrees that the nature of the threat associated with a facility is important in determining what measures and activities the facility should consider implementing to satisfy certain RBPSs. The Department has inserted a statement making this point more clearly in the Introduction to the final Guidance. As the threat facing the facility is only one factor in determining whether or not a given metric is appropriate for the facility, however, it is not possible to narrow down the specific security issues to which each individual metric will universally apply.

The Department also recognizes that a facility which possesses only a single type of security concern (e.g., theft/diversion) is likely to have a justifiably different approach to

security than a facility with a different security issue or issues. In light of this, the Department already had included in the draft Guidance a discussion of different measures that are typically associated with individual security issues in the "General Considerations for Selecting Security Measures to Comply with CFATS" section of the Guidance.

Comment: One commenter noted that many metrics overlap or are repetitive and that DHS should review the Guidance to eliminate repetitiveness and ensure consistency.

Response: In the final Guidance, the Department has done its best to eliminate any repetitive metrics and, as stated above, has corrected certain inconsistencies that were found in the draft Guidance.

Comment: For certain RBPSs, the expected target level (i.e., metric) is the same for all tiers. One commenter alleges that this contravenes the risk-based approach the Department is required by law to follow.

Response: The CFATS regulations, including the RBPSs, do incorporate the risk-based approach required by Section 550. CFATS divides the regulated community of high-risk facilities into four risk-based tiers, with higher levels of compliance with the RBPSs expected from higher risk facilities. See, e.g., 6 CFR § 27.230(a)("acceptable layering of measures to meet [the RBPS] will vary by risk-based tier"). That does not mean, however, that it is necessary or appropriate for every security measure or every metric suggested in the Guidance to be separate and distinct for all four tier levels. While some specific options or specific metrics for certain elements of a given RBPS may be appropriate for multiple tiers, the approaches to satisfying the RBPSs discussed in the Guidance certainly are risk-based. Moreover, as stated previously, none of the security measures or metrics discussed in the Guidance are required for any tier level. Thus, even where the Guidance suggests that a given security measure or metric could be considered by the facilities in more than one tier, any facility that wishes to include other security measures or metrics in its SSP, which the facility believes are appropriate to its tier level, is free to do so, provided that it can demonstrate to DHS how its SSP satisfies the applicable RBPSs. Accordingly, the Department did not modify the Guidance based on this comment.

Comment: One commenter questioned whether some of the RBPS 1 (Restrict Area Perimeter) metrics on vehicle barriers and monitoring and surveillance are realistic for Tier 4.

Response: The Department believes that the Tier 4 metrics for RBPS 1 are realistic and appropriate, and the Department has not modified the Guidance based on this comment.

Comment: One commenter noted that Metric 4.2 implies K-rated crash barriers or other physical barriers are needed even if a site has natural barriers that could prevent an attack.

Response: DHS agrees that, depending on the circumstances, natural barriers can be effectively used to deter or prevent unauthorized vehicles from entering a facility's perimeter and has amended the language of Metric 4.2 to acknowledge this.

Comment: Two commenters expressed concern over the level of detail in Metric 5.2. In particular, they believe that the "Know Your Customer" metrics are too detailed, and seem to imply that a company both needs to know where its product goes after its first customer and must verify the end use of its product.

Response: Metric 5.2 specifically states that the "know your customer program" "*may* include…." (Italics added.) The idea that a facility should be able to verify its product's use throughout the value chain, all the way to the end user, is simply a suggestion for facilities to consider and not a requirement. Accordingly, the Department did not change the Guidance based on this comment.

Comment: One commenter suggested that DHS change Metric 9.3, since not all sites will have automated control systems.

Response: Metric 9.3 expressly acknowledges that facilities can have appropriate response programs without using an automated control system. Specifically, it states that "automated control system *or other process safeguards.*" (Italics added.) Thus, the Department believes there is no need to amend the Guidance based on this comment.

Comment: One commenter suggested that the Department needs to better differentiate between RBPS 15 (Reporting of Significant Security Incidents) and RBPS 16 (Significant Security Incidents and Suspicious Activities).

Response: Reporting of significant security incidents is both the focus of RBPS 15 and one of the activities addressed in RBPS 16. Measures used to address RBPS 15 thus could be used to comply with portions of RBPS 16. Since the CFATS regulations address these two standards individually, however, DHS addresses them separately in the Guidance despite their partial overlap. Accordingly, DHS did not revise the Guidance based on this comment.

Comment: One commenter stated that DHS should suggest alternative identification verification methodologies other than the Transportation Worker Identification Credential (TWIC) and should remove language that implies TWIC is a widely applicable option for RBPS 5 (Shipping, Receipt, and Storage) compliance, as TWIC is not widely available for use in the CFATS context.

Response: Throughout the discussions on identification verification contained in RBPS 5 and elsewhere in the Guidance, the Department explicitly stated that a facility can choose from a wide variety of approaches to comply with identity verification and personnel surety standards, and that the use of TWIC cards is simply one of many options that a facility may wish to consider. As stated in the preamble to the CFATS IFR, the use of a TWIC card or other valid DHS credentials (e.g., a hazardous materials endorsement (HME) license, NEXUS card, Free and Secure Trade (FAST) credential) for CFATS purposes can help minimize redundant background checks and reduce the overall burden on regulated facilities and the employees and contractors who work there. See 72 FR 17709 (April 9, 2007). Accordingly, DHS did not change the Guidance based on this comment.

Comment: Two commenters commented on the recommendations regarding on-site parking restrictions, asserting that the Department's recommendation that facilities minimize onsite parking fails to take into consideration the implications of offsite parking on employee safety. One commenter suggested that the Department revise Metric 3.3 to allow onsite parking in cases where the parking lot is not a restricted area.

Response: The Department agrees with the commenters' suggestion that broader onsite parking may be appropriate in certain circumstances so long as certain compensating security measures are in place (e.g., designated parking areas are a sufficient standoff distance from all critical assets). DHS has revised Metric 3.3 to account for this.

Comment: One commenter stated that the failure to mention Inherently Safer Technology (IST) in the Guidance was inexcusable.

Response: While facilities may voluntarily choose to consider IST solutions as part of their overall security approach, the examination or implementation of IST is not required under CFATS to satisfy the RBPSs and thus is not addressed in the Guidance. No change to the Guidance based on this comment is warranted.

Comment: One commenter stated that the regulations should not have exemptions excluding thousands of chemical facilities such as water treatment facilities.

Response: This comment concerns the CFATS regulations, and by implication the statutory exemptions mandated by Section 550 of the authorizing statute, and thus is beyond the scope of this Guidance. Accordingly, no response is necessary.

Comment: One commenter stated that the Metric 3.2 requirement that personnel and/or visitors be escorted or continuously monitored when at the facility is unnecessary, not

feasible, and offers no meaningful security benefit, and that DHS should adopt the TWIC approach which limits monitoring and escorting to select sensitive areas of the facility.

Response: The commenter does not correctly state the target set by Metric 3.2, and thus no change to Metric 3.2 is required. In addition, the RBPSs themselves (e.g., RBPS 3; RBPS 12) generally are consistent with the TWIC approach to access of individuals to restricted areas.

Comment: One commenter requested that the Guidance provide additional clarification on the role of the Site Security Officer (SSO). Specifically, the commenter inquired as to whether or not the SSO can be someone who has other responsibilities as well (e.g., a safety professional). The commenter also recommended that DHS define SSO responsibilities for the various Tier levels. Another commenter believed that the recommendations made in regard to RBPS 17 (Officials and Organization) do not apply to the industrial gas industry where positions like SSO are addressed at a corporate level.

Response: The draft Guidance already explicitly stated that the SSO can be someone with additional, non-security responsibilities. In regard to defining SSO responsibilities by facility tier level, the Department believes the basic responsibilities of an SSO generally will not vary significantly based on the tier. As to the location of an SSO or other security managers, the Guidance already explicitly stated that an SSO can be located offsite and be responsible for multiple facilities. This holds true for all types of facilities, including industrial gas facilities. (DHS notes, however, that, for purposes of consistency with the CSAT tools, the titles “SSO” and “Assistant SSO” have been changed in the final Guidance to “Facility Security Officer (FSO)” and “Assistant FSO,” respectively.)

Comment: One commenter noted that many facilities do not have room for the standoff distances recommended in Metric 1.3.

Response: Since Metric 1.3 explicitly acknowledges that a facility may use “alternative protective means” in place of standoff distances if it so chooses, no change to the Guidance is needed.

Comment: One commenter noted that Metric 4.3, which recommends intrusion detection systems (IDS) or video surveillance around 100 percent of the facility perimeter, contradicts Metric 1.4, which recommends IDS or video surveillance around 100 percent of the facility perimeter or the perimeter around critical assets.

Response: DHS has resolved the internal inconsistency between Metric 1.4 and Metric 4.3. The final Guidance now states that a facility should consider using intrusion detection or video surveillance around 100 percent of the facility perimeter or the perimeter around critical assets.

Comment: One commenter suggested that DHS should expand the means to fulfill Metric 4.4 to include electronic surveillance monitored by employees or third party vendors, as many facilities do not have security operations centers.

Response: Metric 4.4 discusses a security operations center for Tiers 1 and 2 only, which the Department believes is an appropriate option for facilities in the two highest risk tiers to consider. No additional changes are warranted.

Comment: One commenter requested that DHS explain how it may apply RBPS 19 ("Address any additional performance standards the Assistant Secretary may specify").

Response: At this time, the Department has not identified any additional performance standards that regulated facilities must comply with pursuant to RBPS 19. If the Department identifies any new performance standards, it will notify the regulated community by publication in the *Federal Register*. DHS has added a footnote clarifying this to the introductory chapter of the Guidance.

Comment: One commenter asserted that the four-tier system is inadequate to capture the different hazards facing the varied facilities of the chemical industry and may result in little compliance flexibility.

Response: This comment concerns the four-tier system created by the CFATS regulations, and thus is beyond the scope of this Guidance. Accordingly, no response is necessary.

Comment: One commenter recommended multiple revisions to the chapter on RBPS 1 (Restrict Area Perimeter). First, the commenter stated that chain link fences are not good security, and that the Guidance should recommend, at a minimum, the use of rigid metal mesh fences. Second, the commenter stated that the Guidance failed to consider bullet-resistant barriers or attempts to tunnel under the external perimeter. Third, the commenter asserted that K ratings for vehicle barriers are being replaced by new standards, and that the Guidance may want to incorporate the newer standards.

Response: The Department believes that there are a wide variety of activities that a facility can use to effectively meet RBPS 1, many of which are already described in the Guidance. The Department did not find it necessary to amend the Guidance to specifically include rigid metal mesh fences, bullet-resistant barriers, and anti-tunneling measures among the examples already provided in the Guidance that a facility may wish to consider when determining its comprehensive, layered security posture.

In regard to the K rating comment, the specific references to K ratings contained in the metrics have been removed from the text of the final Guidance as part of the effort to

remove numerical or other specific metrics that may appear prescriptive. However, the discussion of K ratings contained in Appendix C has been retained, as it may prove useful to facilities that are attempting to identify appropriate vehicle barriers for use as part of their SSPs.

Comment: One commenter noted that at least one additional resource noted in Appendix C contained a link to a commercial enterprise, and suggested that DHS remove it.

Response: The Department agrees with the commenter and has removed all resources that are linked to commercial enterprises. Moreover, nothing in the draft or final Guidance should be taken as an explicit or implicit endorsement of any specific product or manufacturer.

Comment: One commenter suggested that the Guidance should explicitly provide a "safe harbor" stating that if a facility follows the Guidance it will be in compliance with CFATS.

Response: As already stated in the Guidance, while a facility meeting all of the relevant metrics contained in the Guidance may well be determined to be in compliance with the CFATS RBPSs, the levels of performance that a facility must achieve to be in compliance will be unique for each facility based on its risk profile. DHS will examine each facility's compliance status comprehensively on a case-by-case basis taking into account all relevant facts and circumstances.

Comment: One commenter noted that Appendix B (RBPS Metrics by Tier) would be a worthwhile tool and should be included in the final Guidance.

Response: The Department agrees, and now that the metrics language for all RBPSs has been finalized, has inserted the complete list of metrics into Appendix B of the final Guidance.

Comment: One commenter questioned whether RBPS 4 (Deter, Detect, and Delay) is applicable to the sabotage threat scenario.

Response: Depending on the security measures and activities employed, all threats can be deterred, detected, and delayed to some degree, including sabotage. Thus, no change to the Guidance is necessary.

Comment: One commenter asked what a "psychological barrier" is.

Response: The Guidance does not mention "psychological barriers," but rather states that barriers can serve as "psychological deterrents" (i.e., can convince adversaries that an asset is not worth attacking). The draft Guidance already provided information on various types of barriers, all of which can serve as psychological deterrents if used appropriately, in the chapter on RBPS 4 (Deter, Detect, and Delay), as well as in several other chapters and Appendix C to the Guidance Additional changes to the Guidance are not warranted based on this comment.

Comment: A commenter recommended the following changes to Table 22 regarding the roles and responsibilities of members of the facility's security organization: (1) change the term "internal audit" to "security audit and/or compliance review," since "internal audit" usually refers to financial audits; (2) add "and exercise" to "planning and conducting security drills;" (3) add "ensuring adequate budget" to the facility manager's roles; and (4) add "Ensuring the conduct of comprehensive, thorough and timely investigation of security incidents by personnel who possess the appropriate competencies and training" to the facility manager's roles.

Response: The Department agrees with suggestions (1), (2) and (4) above and has amended Table 22 in the final Guidance accordingly. The Department disagrees with the recommendation to add "ensuring adequate budget," since the Guidance already states that the facility security manager should "ensure adequate resources."

Comment: One commenter suggested that the Department may want to include more discussion of audits, such as the frequency and timing of audits, and who should conduct an audit.

Response: Pursuant to 6 CFR § 27.225(e), a facility must audit its SSP annually. Who conducts the audit is up to the facility. Note, however, that the chapter on RBPS 17 (Officials and Organization) already provides suggestions for consideration regarding who should be responsible for conducting the audit. The Department did not modify the Guidance based on this comment.