Protecting Critical Infrastructure (2:15pm – 3:15pm)

Attached are three documents that relate to the newly released BPATS (Best Practices for Anti-Terrorism Security) for evaluating security at Metropolitan Commercial Office Buildings.

The three documents are:

- A one-page summary of the BPATS.
- A listing of the BPATS common security practices.
- A field guide for the BPATS.

Additional information about this new tool and how to obtain it is on the government’s program website at www.safetyact.gov.
Background

The Department of Homeland Security (DHS) has national leadership responsibilities for managing risks involving critical infrastructure, key resources, and events. DHS has identified commercial facilities as key assets in the critical infrastructure/key resource sector and encourages the widespread deployment of effective anti-terrorism technologies. Building security programs for commercial facilities can be considered a Qualified Anti-Terrorism Technology (QATT) and may receive designation under the Support Anti-terrorism by Fostering Effective Technologies Act (SAFETY Act) of 2002 as part of the Homeland Security Act of 2002, codified at 6 U.S.C. §441-444. The SAFETY Act provides three levels of liability protections to incentivize the development and deployment of QATs that could significantly reduce the risks or mitigate the effects of large-scale terrorist events. More information about the SAFETY Act is available at https://www.safetyact.gov/.

DHS’s Science and Technology Directorate (S&T) worked in partnership with the National Institute for Building Sciences (Institute) to help building owners and managers identify a set of best operational security practices for metropolitan commercial office buildings, referred to as Best Practices for Anti-Terrorism Security (BPATS) and a corresponding web-based methodology for performing security assessments on commercial buildings. Each of the common security practices has several specific, tactical-level security actions, procedures, methods, equipment or systems related to preparing for, preventing, mitigating and recovering from acts of terrorism. The online BPATS Assessment Tool and field guide provide a recommended process that can be used to improve the content and persuasiveness of assessments. A building owner/operator may wish to consider these practices when developing his/her anti-terrorism security program.

Validation

Through a series of pilot tests with the Institute, S&T refined and validated both the BPATS and the Assessment Tool to ensure that an assessor would be able to provide feedback that would help a building owner make informed risk-based decisions. While this is a comprehensive set of BPATS, it also is scalable; a facility would not be required to satisfy all of the BPATS. Rather, building owners/operators should consider the appropriate level of security measures necessary to mitigate the risk to their facilities. This method will also help a building owner identify the steps taken to address the risk assessment, as part of an application for SAFETY Act protections, should the building owner wish to apply.

Availability and Use

The BPATS Tool and supporting materials are available at https://bpatsassessmenttool.nibs.org/.

Building owners/operators and assessors may apply for access to the web-based Tool online. To ensure that applications of the BPATS are consistent and thorough, Assessors must identify their security credentials to obtain training and to use the web-based Tool.

Access to the BPATS Tool is free and training is also available free of charge in both live and on-line versions.

To learn more about the BPATS Tool, visit: https://bpatsassessmenttool.nibs.org
BEST PRACTICES FOR ANTI-TERRORISM SECURITY (BPATS) LIST FOR COMMERCIAL OFFICE BUILDINGS

BPATS 1.1 Top Management Commitment
BPATS Assessment Tool Flowchart
BPATS Assessment Tool Input Screen

DHS Office of SAFETY Act Implementation
2018-11
Table of Contents

Layout of the Best Practice Listing .......................................................................................... 2

1. Security Program Charter ..................................................................................................... 3
   1.1 Top Management Commitment ....................................................................................... 3
   1.2 Policy ............................................................................................................................. 4
   1.3 Scope and Objectives ...................................................................................................... 5

2. Strategic Planning ................................................................................................................ 6
   2.1 Risk Assessment ............................................................................................................ 6
   2.2 Risk Awareness ............................................................................................................. 8
   2.3 Incident Preparedness .................................................................................................... 9
   2.4 Incident Response and Recovery .................................................................................. 12
   2.5 Continuity of Operations .............................................................................................. 14

3. Administrative Controls ...................................................................................................... 15
   3.1 People Surety ............................................................................................................... 15
   3.2 Identification and Verification ..................................................................................... 17
   3.3 Information Security .................................................................................................... 19

4. Security Systems ................................................................................................................ 21
   4.1 Command Center ......................................................................................................... 21
   4.2 Systems ......................................................................................................................... 22
   4.3 Redundancy and Diversity ......................................................................................... 26
   4.4 Maintenance ................................................................................................................ 27

5. Communication and Notification ....................................................................................... 28
   5.1 Policies and Procedures ............................................................................................... 28
   5.2 Signage and Announcements ....................................................................................... 30

6. Defensible Space Design .................................................................................................... 31
   6.1 Physical Structure ........................................................................................................ 31
   6.2 Protected Areas ........................................................................................................... 33
   6.3 Controlled and Restricted Areas ................................................................................ 35
   6.4 Accessories .................................................................................................................. 36
   6.5 Utility Systems and Equipment .................................................................................. 37

7. Performance Evaluation ...................................................................................................... 38
   7.1 Exercising and Testing ............................................................................................... 38
   7.2 Evaluation .................................................................................................................... 39
Layout of the Best Practice Listing
The following taxonomy has been established for the Best Practices for Anti-Terrorism Security (BPATS):

- At the highest level there are 7 Practice Categories used to organize the 24 BPATS. Each Practice Category contains two to five related Best Practices for Anti-Terrorism Security or BPATS. There are a total of 24 BPATS.
- Under each individual BPATS, there are three to 60 associated Common Security Practices for a total of 411 Common Security Practices.

The following figure depicts the layout of the best practice list. The Practice Category is first listed followed by the Best Practices in that category. For each Best Practice, the Title, Scope, Best Practice Statement, and Common Security Practices are enumerated.

1. Security Program Charter ①

1.1 Top Management Commitment ②

<table>
<thead>
<tr>
<th>Scope:</th>
<th>Addresses practices related to top management’s commitment to establish, implement, maintain, and continuously improve the site security program, especially with respect to program policy, scope, and objectives. ③</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best Practice:</td>
<td>Top management demonstrates a commitment to the security program by: (a) developing, reviewing, updating, and approving the program policy and issuing sufficient authorizations; (b) ensuring resources (human, financial, material) are provided to establish, implement, and maintain the security program in accordance with the facility’s risk assessment and the security program plan’s scope and objectives; (c) appointing an individual to lead the program; (d) assigning an individual to conduct periodic, independent reviews of the program; (e) ensuring relevant security information is communicated to management, employees, tenants, and visitors, as necessary; and (f) supporting employees in the implementation of the security program. ④</td>
</tr>
<tr>
<td>Common Security Practices ⑤</td>
<td>A top manager is identified (e.g., a facility owner, operator, or board director) willing to take responsibility for security policy and implementation. Sufficient resources are provided to establish, implement, maintain, and improve the organization’s security program.</td>
</tr>
<tr>
<td>1.1.01</td>
<td>Top management endorses the security program policy.</td>
</tr>
<tr>
<td>1.1.02</td>
<td></td>
</tr>
</tbody>
</table>

Figure 1: Layout of the BPATS Listing

① This section indicates the practice category. There are seven categories.
② This section indicates the title of the best practice. There are 24 best practices.
③ This statement addresses the scope of the security practices.
④ This section is the Best Practice Statement. It identifies the outcome specified by the best practice (i.e., the requirements).
⑤ This section identifies Common Security Practices. The security practices are suggested anti-terrorism actions, procedures, methods, or systems that execute the outcome specified by the best practice. Note that the common security practices are not all encompassing.
1. Security Program Charter

1.1 Top Management Commitment

**Scope:** Addresses practices related to top management’s commitment to establish, implement, maintain, and continuously improve the site security program, especially with respect to program policy, scope, and objectives.

**Best Practice:** Top management demonstrates a commitment to the security program by: (a) developing, reviewing, updating, and approving the program policy and issuing sufficient authorizations; (b) ensuring resources (human, financial, material) are provided to establish, implement, and maintain the security program in accordance with the facility's risk assessment and the security program plan's scope and objectives; (c) appointing an individual to lead the program; (d) assigning an individual to conduct periodic, independent reviews of the program; (e) ensuring relevant security information is communicated to management, employees, tenants, and visitors, as necessary; and (f) supporting employees in the implementation of the security program.

<table>
<thead>
<tr>
<th>Common Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.1.01</strong></td>
</tr>
<tr>
<td><strong>1.1.02</strong></td>
</tr>
<tr>
<td><strong>1.1.03</strong></td>
</tr>
<tr>
<td><strong>1.1.04</strong></td>
</tr>
<tr>
<td><strong>1.1.05</strong></td>
</tr>
<tr>
<td><strong>1.1.06</strong></td>
</tr>
<tr>
<td><strong>1.1.07</strong></td>
</tr>
<tr>
<td><strong>1.1.08</strong></td>
</tr>
<tr>
<td><strong>1.1.09</strong></td>
</tr>
<tr>
<td><strong>1.1.10</strong></td>
</tr>
</tbody>
</table>
# 1.2 Policy

**Scope:** Addresses practices related to the site security program policy, which provides the procedural framework for making security decisions, including a strategic direction and principles of action.

**Best Practice:** The site’s security program policy: (a) provides a framework for setting anti-terrorism security objectives; (b) is based on the facility’s risk assessment; (c) establishes the entity’s commitment to continuous improvement of the security program using measurable indicators where they are applicable; (d) is reviewed on a regular basis; (e) ensures employee adherence to security program policies; (f) is made available to authorized parties; (g) is communicated to all stakeholders; and (h) is reviewed at regular intervals (no less than annually or when significant changes occur).

## Common Security Practices

<table>
<thead>
<tr>
<th>1.2.01</th>
<th>The security policy complies with applicable laws, standards, and strategies based on the site’s current threat environment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.02</td>
<td>Consider design-basis threat scenarios in setting the site’s security program policy.</td>
</tr>
<tr>
<td>1.2.03</td>
<td>Periodically review that the security program policy, strategies, plans, and solutions are in line with the security program’s requirements.</td>
</tr>
<tr>
<td>1.2.04</td>
<td>Consider subjecting employees that do not adhere to the security program policy to administrative (e.g., additional training or reassignment) or disciplinary action.</td>
</tr>
</tbody>
</table>
### 1.3 Scope and Objectives

**Scope:** Addresses practices that relate to establishing, implementing, and maintaining the scope and objectives of the security program. Scope is defined as those aspects of site operations to which the site security program shall apply. Objectives are defined as the desired outcomes of successful implementation of the site security program.

**Best Practice:** The scope and objectives of the security program are taken into account by the site’s capital investment plan and are clearly defined and documented, with regard to the following: (a) requirements of a security program for the facility; (b) roles and responsibilities of senior management, security personnel, facility operations personnel, employees, building occupants, and visitors; (c) the life safety of all occupants; (d) risk tolerance as determined by top management, with input from the security director; (e) statutory, regulatory and contractual requirements; and (f) interests of key stakeholders.

<table>
<thead>
<tr>
<th>Common Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.3.01</strong></td>
</tr>
<tr>
<td><strong>1.3.02</strong></td>
</tr>
<tr>
<td><strong>1.3.03</strong></td>
</tr>
<tr>
<td><strong>1.3.04</strong></td>
</tr>
<tr>
<td><strong>1.3.05</strong></td>
</tr>
</tbody>
</table>
2. Strategic Planning

2.1 Risk Assessment

**Scope:** Addresses practices that relate to conducting a risk assessment for the site and its operations.

**Best Practice:** A risk assessment that addresses threats, vulnerabilities, and consequences has been performed for the facility by a qualified individual. It is used to develop and implement the security program. The risk assessment provides a design basis threat for each threat scenario developed and prioritizes risk by considering how each asset is impacted by each threat scenario. The risk assessment is regularly reviewed (no less than annually or when significant changes occur) and is updated based on review.

<table>
<thead>
<tr>
<th>Common Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2.1.01</strong> Ensure objectivity of the risk assessment process by using an independent outside party to either conduct or validate the assessment.</td>
</tr>
<tr>
<td><strong>2.1.02</strong> Base all security program plans and procedures relating to preparedness, incident response and recovery, and continuity of operations, on the results of the facility's risk assessment.</td>
</tr>
<tr>
<td><strong>2.1.03</strong> Base the risk assessment for the facility on a DHS-approved risk management framework, such as the National Infrastructure Protection Plan (NIPP).</td>
</tr>
<tr>
<td><strong>2.1.04</strong> Quantify the risk and resilience of the facility. Reference DHS Science &amp; Technology Building and Infrastructure Publication-04 (BIPS-04) &quot;Integrated Rapid Visual Screening of Buildings&quot;.</td>
</tr>
<tr>
<td><strong>2.1.05</strong> A Risk Assessment has been conducted. Reference: DHS Science and Technology's Building and Infrastructure Protection Series (BIPS) publication BIPS-06 &quot;Reference Manual to Mitigate Potential Terrorist Attacks Against Building&quot;.</td>
</tr>
<tr>
<td><strong>2.1.06</strong> Incorporate assessments of threats (likelihood), vulnerabilities (weak points), and consequences (impact) when conducting risk assessments. Use, when possible, information collected from actual prior incidents to better develop appropriate responses. Determine security countermeasures for identified risks and prioritize them relevant to their criticality and probability of occurrence.</td>
</tr>
<tr>
<td><strong>2.1.07</strong> The risk assessment methodology prioritizes risk by considering how each asset (e.g., people, infrastructure, systems, etc.) is impacted by each threat scenario.</td>
</tr>
<tr>
<td><strong>2.1.08</strong> Revise all security program plans and procedures periodically or particularly when threats, vulnerabilities, or consequences of a terrorist attack change.</td>
</tr>
<tr>
<td><strong>2.1.09</strong> Analyze the activities and operations in the surrounding area of the facility (e.g., airports, chemical plants, government buildings, pipelines, rail lines, transportation/subway terminals, public assembly venues, etc.) to determine if there is any potential for them to change security risks to the building. Include this analysis in all risk assessments.</td>
</tr>
<tr>
<td><strong>2.1.10</strong> Get input from the site's insurance broker and a cross-section of the occupants of the building when performing the risk assessment.</td>
</tr>
<tr>
<td><strong>2.1.11</strong> Meet with adjacent facilities regularly to discuss local and common security issues, and to share information. Include this information as part of the risk assessment.</td>
</tr>
<tr>
<td><strong>2.1.12</strong> The following inputs were considered in the risk assessment: the probability of an event; the magnitude and severity of the event; the time available for public warning; the probable location(s) of the event, the potential size of the affected area, the duration of consequences, and potential cascading effects.</td>
</tr>
<tr>
<td><strong>2.1.13</strong> Be aware of materials already in place at the building that could be leveraged for illicit purposes (e.g., flammable materials, hazardous chemicals, etc.). Include this information in the vulnerability part of the risk assessment.</td>
</tr>
<tr>
<td><strong>2.1.14</strong> Consider the impact on facility operations if all essential computer system resources (command, control, and financial computer systems) are disconnected from the internet and public access.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td><strong>2.1.15</strong></td>
</tr>
<tr>
<td><strong>2.1.16</strong></td>
</tr>
<tr>
<td><strong>2.1.17</strong></td>
</tr>
<tr>
<td><strong>2.1.18</strong></td>
</tr>
<tr>
<td><strong>2.1.19</strong></td>
</tr>
<tr>
<td><strong>2.1.20</strong></td>
</tr>
</tbody>
</table>
### 2.2 Risk Awareness

**Scope:** Addresses practices that relate to establishing, implementing, and maintaining situational awareness of risks to the facility

**Best Practice:** Awareness of foreseeable risk (threats, vulnerabilities, and consequences) is maintained in accordance with the security program policy, scope, and objectives. Efforts are taken to identify changes to threats, vulnerabilities, and consequences. When changes are identified, the security program is updated as necessary.

#### Common Security Practices

| 2.2.01 | Immediately conduct a system-wide risk assessment when a change in conditions warrants it (e.g., intelligence indicates a change in threats). |
| 2.2.02 | Identify a liaison from the security staff to maintain regular communication with DHS, local law enforcement and FBI, federal and state homeland security advisors, public health organizations, and industry organizations. Regularly exchange information, threat conditions, suspicious activity, and investigative support. |
| 2.2.03 | Monitor the National Terrorism Advisory System (NTAS) and Maritime Security (MARSEC) threat levels and take appropriate precautions consistent with the risk assessment. |
| 2.2.04 | Participate in established communications network with neighboring facilities or local police and fire departments, such as CEAS (Corporate Emergency Access System). Participate in established REISAC (Real Estate Information Sharing and Analysis Center) through subscription to e-mail notifications. |
| 2.2.05 | Maintain awareness of changing security risks to the site. When addressing changing security risks, always consider the following: the impact of nearby facilities and properties (e.g., government buildings, airports, stadiums, convention centers, industrial plants, pipelines, railroads, etc.); the impact on the facility if neighboring facilities are attacked. This is particularly important if a nearby facility is attractive to terrorist activity (e.g., critical infrastructure, government, military, recreational areas, transportation, utilities, etc.); and the potential impact of identified or emerging risks to the facility. |
| 2.2.06 | Monitor nearby land use and future development plans, particularly those that are on the immediate perimeter of the site. Monitor nearby building use changes (i.e. office to school facility) or change in tenant profile for potential threat either in building or nearby. |
| 2.2.07 | Maintain up-to-date contact information for internal stakeholders (e.g., employees, tenants, etc.) and external stakeholders (e.g., first responders, government officials, etc.) for potential outreach and networking and sharing of information. |
| 2.2.08 | Deter or prevent the use of photography of sensitive areas and closely monitor photography in public areas (i.e., tourist photogenic areas) in accordance with site risk tolerance. |
| 2.2.09 | Establish a Common Operating Picture by integrating data from security system elements (e.g., access control, CCTV, security alarms, fire/life safety systems, HVAC systems, Chemical Biological Nuclear Radiological and Explosive (CBRNE) systems, etc.). |
### 2.3 Incident Preparedness

**Scope:** Addresses practices that relate to developing and documenting site security plans that address preparing for, mitigating and deterring, responding to, and recovering from an act of terrorism.

**Best Practice:** Plans have been established, implemented, and maintained to support prevention, mitigation, response, recovery, business continuity operations, and drills and exercises in connection with a terrorist attack. These plans are consistent with the findings of the risk assessment. The plans are documented and include documented agreements with first responders. The plans are developed by qualified individuals.

#### Common Security Practices

<table>
<thead>
<tr>
<th>2.3.01</th>
<th>Use site risk assessments to develop and maintain incident management plans and response procedures.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.02</td>
<td>Include input from a cross section of employees, building tenants, vendors, long-term contractors, and security personnel when developing security plans. Invite law enforcement and first responders to participate.</td>
</tr>
<tr>
<td>2.3.03</td>
<td>Identify potential incident commanders either by position type or name. Require designated incident commanders to become familiar with the NIMS.</td>
</tr>
<tr>
<td>2.3.04</td>
<td>Interdependencies and resource availability are considered during formulations of plans and procedures.</td>
</tr>
<tr>
<td>2.3.05</td>
<td>Establish, implement, and maintain policies and procedures to activate an emergency operations command center(s) and initiate the incident command system.</td>
</tr>
<tr>
<td>2.3.06</td>
<td>Establish, implement, and maintain incident command procedures that include a unified command plan with appropriate stakeholders (e.g., local law enforcement, emergency responders, or other government agencies). Appropriate local law enforcement personnel and emergency responders should know the names of and have contact information for the organization's security team and the appropriate members of the incident command structure.</td>
</tr>
<tr>
<td>2.3.07</td>
<td>Establish, implement, and maintain a process for the reporting of suspicious activities, objects, and occurrences to appropriate security, building management, or appropriate authorities. Ensure procedures exist for questioning people acting suspiciously or violating security regulations, and denying access to those persons.</td>
</tr>
<tr>
<td>2.3.08</td>
<td>Establish, implement, and maintain procedures for periodic inspections of protected and restricted areas in the facility, including lockers and storage areas, at higher threat or other conditions as specified in the facility's risk assessment.</td>
</tr>
<tr>
<td>2.3.09</td>
<td>Establish, implement, and maintain a response plan. Address lifesaving and mitigation-of-impact procedures, which should be taken immediately after an incident (e.g., restricting entrance to the impacted areas, protecting undamaged property, preventing tampering of the scene, etc.). Model the plan on the National Incident Management System (NIMS). Include directions for restricting entrance to the impacted areas that will protect the life of survivors and responders, protect undamaged property, prevent tampering of the scene, and in general, prevent further negative impacts.</td>
</tr>
<tr>
<td>2.3.10</td>
<td>Establish, implement, and maintain an occupant emergency plan that directs occupants on how to react to emergency situations.</td>
</tr>
<tr>
<td>2.3.11</td>
<td>Establish, implement, and maintain a communication and notification plan that covers voice, data, and video transfer of information related to safety and security. Provide a simple and straightforward means for people to send and receive information regarding a potential threat or an emergency.</td>
</tr>
<tr>
<td>2.3.12</td>
<td>Establish, implement, and maintain a liaison with First Responders concerning decontamination plans (e.g., for chemical, biological, radiation, and nuclear [CBRN] materials) for the building, taking into account neighboring infrastructure and facilities. Ensure the buildings Incident response plans do not conflict with the plans of the First Responders.</td>
</tr>
<tr>
<td>2.3.13</td>
<td>Establish, implement, and maintain emergency procedures that include contingencies for the loss of power, heating, cooling, water and sewage and other vital utilities.</td>
</tr>
<tr>
<td>2.3.14</td>
<td>Establish, implement, and maintain an evacuation plan for the facility. Ensure plans address the needs of special needs staff and occupants (e.g., persons with hearing or visual impairments, persons with poor reading skills, or non-English speakers). Coordinate site evacuation plans with commercial tenant plans and all neighboring facilities; meet annually to exercise and update plans.</td>
</tr>
<tr>
<td>2.3.15</td>
<td>Establish, implement, and maintain procedures for shelter-in-place or safe room situations. Indicate which emergency situations (e.g., active shooter) necessitate sheltering-in-place or moving to safe room locations.</td>
</tr>
<tr>
<td>2.3.16</td>
<td>Establish, implement, and maintain written procedures for the HVAC (heating, ventilation, and air-conditioning) system control (e.g., emergency shutdown, set for 100 percent recirculated air, etc.).</td>
</tr>
<tr>
<td>2.3.17</td>
<td>Establish, implement, and maintain a recovery plan. Address procedures for restoring mission critical functions once incident response has been completed. Consider including actions such as: reopening undamaged areas, reduction in services, and activation of memoranda of understanding.</td>
</tr>
<tr>
<td>2.3.18</td>
<td>Establish, implement, and maintain a plan for post-incident employee counseling (incident stress management, psychological services, and family assistance).</td>
</tr>
<tr>
<td>2.3.19</td>
<td>Establish, implement, and maintain contingency plans to provide for the welfare of employees and their families, such as assistance with overnight shelter and food.</td>
</tr>
<tr>
<td>2.3.20</td>
<td>Establish, implement, and maintain organizational plans that address security procurement, workplace violence, prohibited items and substances, and key control.</td>
</tr>
<tr>
<td>2.3.21</td>
<td>Identify primary and alternate evacuation routes and assembly locations (muster points).</td>
</tr>
<tr>
<td>2.3.22</td>
<td>Emergency management and site security personnel and other authorized users have immediate access to all security and emergency response plans (e.g., emergency plans, emergency instructions, and building plans, the facility security plan, and contact and communication information).</td>
</tr>
<tr>
<td>2.3.23</td>
<td>Set in place emergency response memorandums of agreement or mutual aid agreements.</td>
</tr>
<tr>
<td>2.3.24</td>
<td>Document areas within the building with uninterruptible power supply (UPS) and batteries. Identify their locations and make sure their locations are known by appropriate response personnel.</td>
</tr>
<tr>
<td>2.3.25</td>
<td>Document locations in the facility where chemicals and other hazardous materials may be found, particularly in chemical storage areas. Mark the entrances to these locations with clear signage. Share this information with appropriate response personnel.</td>
</tr>
<tr>
<td>2.3.26</td>
<td>Document the names and contact information of appropriate law enforcement personnel and emergency responders. When feasible, security personnel and crisis management leaders should be familiar with local law enforcement and emergency response personnel and procedures.</td>
</tr>
<tr>
<td>2.3.27</td>
<td>Coordinate with local agencies the emergency access lanes for fire, police, and emergency medical services (EMS) personnel. In addition, coordinate the location of areas where appropriate response personnel can establish incident command posts.</td>
</tr>
<tr>
<td>2.3.28</td>
<td>Include and maintain in incident plans the contact information and pertinent information for disaster recovery services.</td>
</tr>
<tr>
<td>2.3.29</td>
<td>Coordinate with local agencies the emergency access lanes for fire, police, and emergency medical services (EMS) personnel. In addition, coordinate the location of areas where appropriate response personnel can establish incident command posts.</td>
</tr>
<tr>
<td>2.3.30</td>
<td>Plans include post-event procedures for recording vital information about an incident, actions taken, decisions made, and lessons learned. Include in incident management procedures a requirement to have a post-event debrief to identify lessons learned.</td>
</tr>
<tr>
<td>2.3.31</td>
<td>Invite municipal entities (e.g., fire, local law enforcement) to review and assess building security plans and procedures.</td>
</tr>
<tr>
<td>2.3.32</td>
<td>Ensure all retail occupants are familiar with applicable site security procedures.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>2.3.33</td>
<td>Each facility shall have an armed attacker (active threat armed with any type of weapon (e.g., firearm, knife, explosives, etc.)) preparedness plan, which is to be updated at a minimum every two years, or as needed based upon events/incidents. At a minimum, a plan should comprise the following elements: a. Security Assessments; b. Preparedness; c. Communication; d. Incident Plan (i.e., actions to take during an incident); e. Training and Exercises; f. Post Incident Recovery for Employees and Operations of the property. Note: the plan need not be a standalone document. (Planning and Response to an Active Shooter: An ISC Policy and Best Practices Guide, Nov. 2015.)</td>
</tr>
<tr>
<td>2.3.34</td>
<td>Encourage retail occupants to develop a business continuity plan that is consistent with facility security plans.</td>
</tr>
<tr>
<td>2.3.35</td>
<td>Document the time of the last revision for each security plan used in the site security program.</td>
</tr>
<tr>
<td>2.3.36</td>
<td>Establish an armed attack exercise program. Identify the best training approach for different facility occupants (general public, tenants, facility management, security staff). Conduct different types of exercises according to a group's training needs. (For example: tenants would benefit from participation in discussion-based exercises, such as seminars, or armed attack drills. Employees, facility management and security would benefit from Table Top Exercises and hands-on scenario-based training.) Extend exercise participation opportunities to the external emergency responders likely to support the facility in an active armed attack situation.</td>
</tr>
<tr>
<td>2.3.37</td>
<td>Facility Management (or as coordinated, tenant management) shall provide training, materials, and/or awareness discussions to inform building/facility employees of active shooter preparedness plans as they are updated. Building/facility employees should be aware of the Federally-endorsed run-hide-fight concept. Building/facility employees should be informed of the importance of having a personal plan. New building/facility employees should be given active armed attacker preparedness training during the initial onboarding period.</td>
</tr>
<tr>
<td>2.3.38</td>
<td>Facility management shall collaborate with the facility security provider, on-site law enforcement agencies (if applicable), and first responder agencies likely to address an armed attack situation to confirm local response protocols, identification of potential operational issues that might be encountered or require coordination.</td>
</tr>
</tbody>
</table>
### 2.4 Incident Response and Recovery

**Scope:** Addresses practices and procedures that relate to responding and recovering from an act of terrorism.

**Best Practice:** Appropriate procedures are in place to enable: (a) response for life safety and damage mitigation and (b) resilient recovery. Specific persons (e.g., area captain, marshal, warden, etc.) have been designated, trained, and resourced to conduct such operations, as necessary. Key personnel are cross-trained and procedures are rehearsed. Appropriate liaisons have been established with first responders. Procedures are based on the facility’s risk assessment.

<table>
<thead>
<tr>
<th>Common Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2.4.01</strong> Identify potential incident commanders either by position type or name. Require designated incident commanders to become familiar with the NIMS.</td>
</tr>
<tr>
<td><strong>2.4.02</strong> Designate staff to serve on an emergency response team. Design the team such that it can be scaled to fit the emergency situation as described in the NIMS.</td>
</tr>
<tr>
<td><strong>2.4.03</strong> Maintain and have readily available at the facility a list of employees, tenants, vendors, contractors, and other non-visitor occupants. Ensure the list includes emergency contact information. Keep this list as current as possible always considering the number of facility occupants.</td>
</tr>
<tr>
<td><strong>2.4.04</strong> Inventory emergency equipment and supplies periodically to verify that needed quantities (per risk level) are adequately stocked, available, and within any applicable expiration date.</td>
</tr>
<tr>
<td><strong>2.4.05</strong> Provide in advance a list of special needs people to local first responders (fire and police).</td>
</tr>
<tr>
<td><strong>2.4.06</strong> Get input from local EMS on how to handle medical emergencies in the facility, including advice on where to set up first aid and triage stations and transport sites.</td>
</tr>
<tr>
<td><strong>2.4.07</strong> Plan and test liaison with First Responders and have the capability to share information and data (video feeds) at the Security Operations Center, or facility command center, with first responders and other agencies and entities during emergency response and recovery operations.</td>
</tr>
<tr>
<td><strong>2.4.08</strong> Identify a floor captain or marshal who is responsible for each floor or tenant of the site (whichever is more applicable). The captain or marshal is responsible for implementing each floor's or tenant's appropriate emergency plan, and ensuring that it is carried out properly. In the case of evacuations, check for stay-behinds.</td>
</tr>
<tr>
<td><strong>2.4.09</strong> When necessary, require evacuation of all occupants of the facility without specific emergency related duties.</td>
</tr>
<tr>
<td><strong>2.4.10</strong> Locate and address the needs of people who require special attention during a disaster (e.g., the disabled, people with poor reading skills, non-English speakers, etc.).</td>
</tr>
<tr>
<td><strong>2.4.11</strong> Increase on duty security staff during heightened threat conditions or in response to an incident. Account for additional security staff requirements if reinforcements or relief personnel are needed.</td>
</tr>
<tr>
<td><strong>2.4.12</strong> Locate muster stations in low traffic and fireproof areas near stairwells or freight elevators.</td>
</tr>
<tr>
<td><strong>2.4.13</strong> Recall elevators to the ground floor in the event of an emergency. Use freight elevators for responder staging or evacuation.</td>
</tr>
<tr>
<td><strong>2.4.14</strong> If necessary, control elevators remotely from the command center during an emergency.</td>
</tr>
<tr>
<td><strong>2.4.15</strong> In incident plans, comply with local code for mandatory evacuation due to fire from the affected floor and floors above and below per local code.</td>
</tr>
<tr>
<td><strong>2.4.16</strong> Establish incident response procedures for a kidnapping incident. Up to the limits of the security officer's authority, immediately lockdown the site in the event of a kidnapping and liaison with responding police.</td>
</tr>
<tr>
<td><strong>2.4.17</strong> Inspect public areas in the event of a general bomb threat. Absent positive target identification (PTI) indicators or other credible information, an evacuation may not be appropriate. Evacuate and search any area affected by a specific threat.</td>
</tr>
<tr>
<td>2.4.18</td>
</tr>
</tbody>
</table>
## 2.5 Continuity of Operations

**Scope:** Addresses practices that relate to ensuring the availability of the site’s designated critical functions before, during, and after a terrorist incident.

**Best Practice:** Appropriate procedures are in place or resources are available to ensure the functionality of critical activities of the security program.

<table>
<thead>
<tr>
<th>Common Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2.5.01</strong> Solicit input from the all tenant organizations as to their business continuity requirements.</td>
</tr>
<tr>
<td><strong>2.5.02</strong> Establish, implement, maintain, and exercise COOP plans for critical incident management functions of the facility.</td>
</tr>
<tr>
<td><strong>2.5.03</strong> Identify alternate worksite(s), if needed, to ensure continuity of operational activities.</td>
</tr>
<tr>
<td><strong>2.5.04</strong> Designate an alternate or back up site for continuing critical activities during an incident.</td>
</tr>
<tr>
<td><strong>2.5.05</strong> Create mutual aid and resource sharing programs and agreements with neighboring buildings.</td>
</tr>
<tr>
<td><strong>2.5.06</strong> Conduct a business impact assessment that will help to determine the consequences if operations are disrupted.</td>
</tr>
<tr>
<td><strong>2.5.07</strong> Identify the maximum time between the last backup of critical information and disruption that could eliminate unrecoverable data. Develop procedures to address this potential vulnerability.</td>
</tr>
<tr>
<td><strong>2.5.08</strong> Identify maximum allowable recovery times for critical functions (e.g., restoration of power).</td>
</tr>
<tr>
<td><strong>2.5.09</strong> Create a security culture where all staff knows that backup personnel are designated to execute emergency functions if primary personnel are unavailable or incapacitated.</td>
</tr>
</tbody>
</table>
3. Administrative Controls

### 3.1 People Surety

**Scope:** Addresses practices that relate to ensuring: (a) the quality, competence, and suitability of site security personnel, and (b) the ability of all relevant security and nonsecurity personnel (including staff, tenants, and certain visitors) to implement the security program, as appropriate.

**Best Practice:** Security personnel are qualified and pre-screened (background checks) in accordance with applicable legal requirements and commensurate with the risks identified for the facility. Measures are in place to attract and retain high-performing personnel. Other facility personnel (i.e., employees, vendors, contractors, and site tenants) are trained to implement the security program, as appropriate.

<table>
<thead>
<tr>
<th>Common Security Practices</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.01 Screen all potential security staff to check the applicant's identity, employment history, criminal history, financial history, and overseas activity.</td>
<td></td>
</tr>
<tr>
<td>3.1.02 All security staff is appropriately licensed.</td>
<td></td>
</tr>
<tr>
<td>3.1.03 Create a set of minimum qualifications (knowledge, skills, and abilities) for hiring security staff (e.g., licensing, education requirements, knowledge and application of security practices, skill with security equipment, ability to work independently and as part of a team, ability to communicate, etc.). Consider giving preference to applicants with a college degree, relevant professional certifications, or with a law enforcement background. Ensure factors are consistent with legal requirements.</td>
<td></td>
</tr>
<tr>
<td>3.1.04 Create a list of disqualifying factors that can be used to reject an individual for employment. Ensure factors are consistent with legal requirements.</td>
<td></td>
</tr>
<tr>
<td>3.1.05 Where allowed by law, collect a biometric, typically fingerprints, from security staff employees as a condition of employment.</td>
<td></td>
</tr>
<tr>
<td>3.1.06 Consider hiring a qualified training coordinator that oversees employee security training needs.</td>
<td></td>
</tr>
</tbody>
</table>

**Security Staff – Training**

| 3.1.07 Security staff training meets all jurisdictional training requirements. Consider requiring additional training requirements per quarter that are tailored for the site and include site-specific scenario reviews. |  |
| 3.1.08 Create and maintain a training record for each security staff member. Regularly monitor and track the training record. |  |
| 3.1.09 Provide specialized training to security personnel based on their position requirements. |  |
| 3.1.10 Ensure all security staff training (including refresher training) is tailored to the particular facility (e.g., building specific security policies and procedures, workplace violence, crime prevention measures, suspicious packages, reporting security incidents, proper reporting and response to fires and other emergencies, operational security measures, and appropriate response to incidents per the facility security plan). |  |
| 3.1.11 Consider rewarding members of security staff who complete optional training (e.g., online training modules). |  |
| 3.1.12 Train security staff on the procedures and operation of all screening equipment. |  |
| 3.1.13 Train staff to implement public awareness programs such as DHS's "If You See Something, Say Something:" campaign. |  |
| 3.1.14 Train security staff to identify and question suspicious persons and how to handle unattended, left-behind packages. |  |
| 3.1.15 Train security staff in first aid, cardiopulmonary resuscitation (CPR), and in the use of external defibrillators. |  |
| 3.1.16 Train security staff on the location and use of manual fire-pull stations, fire extinguishers, and stairwell exits on each floor. |  |
### 3.1.17
Train security staff on the safe approach to illegally parked vehicles.

### 3.1.18
Train security staff to implement response plans, specifically their individual roles and responsibilities. Give a copy of the facility's emergency plans and instructions to all new facility employees, preferably at an employee orientation session. Training should include information on the specific protective measures that the facility will implement during an emergency.

### 3.1.19
Train security staff on how to shut off utility services, when appropriate (e.g., emergencies).

### 3.1.20
Train security staff how to recognize official law enforcement uniform and identification badges.

### 3.1.21
Train access control staff in behavioral profiling and identification badge recognition.

### 3.1.22
Offer refresher training for security staff on current principles, practices, and trends in technology.

<table>
<thead>
<tr>
<th>Nonsecurity Staff and Contractors – Hiring, Background, and Qualifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.23 Perform background checks on new frontline operations and maintenance employees, as well as employees and contractors with access to sensitive security information and security critical facilities and systems.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nonsecurity Staff and Contractors – Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.24 Give a copy of emergency plans and instructions, particularly the evacuation plan, to all new employees preferably at an employee orientation session.</td>
</tr>
<tr>
<td>3.1.25 Provide security training on current security matters to top facility managers, including but not limited to, corporate level executives, general managers, and operations managers.</td>
</tr>
<tr>
<td>3.1.26 Train nonsecurity staff to implement response plans, specifically their individual roles and responsibilities (when applicable). Give a copy of facility emergency instructions to all new facility employees, preferably at an employee orientation session.</td>
</tr>
<tr>
<td>3.1.27 Train facility staff, including part-time, adjunct, logistics, and contract employees, to identify suspicious people, objects, and activities.</td>
</tr>
<tr>
<td>3.1.28 Instruct staff to secure sensitive material (e.g., not leaving sensitive items lying on desktops, logging off computers when not present, etc.).</td>
</tr>
<tr>
<td>3.1.29 Train building tenants in the proper use of available emergency equipment, such as fire extinguishers, heart defibrillator, etc. Instruct those not trained not to operate emergency equipment.</td>
</tr>
<tr>
<td>3.1.30 Train all tenants on the use and location of manual fire-pull stations, fire extinguishers, and stairwell exits on each floor.</td>
</tr>
</tbody>
</table>
### 3.2 Identification and Verification

**Scope:** Addresses practices that relate to the identification, verification, and appropriate credentialing of persons and objects on site, as necessary.

**Best Practice:** The identification system clearly identifies and verifies authorized personnel, guests, vehicles, and deliveries, and mitigates system abuse through control measures.

#### Common Security Practices

<table>
<thead>
<tr>
<th>3.2.01</th>
<th>The security office exercises sole control over the facility's identification and verification system (e.g., issuing and revoking identification badges, etc.).</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.02</td>
<td>Issue identification badges containing photographs to building employees, tenants, contractors, cleaning crews, vendors, and temporary employees. Require that all identification badges be displayed at all times and verified to gain access to the building.</td>
</tr>
<tr>
<td>3.2.03</td>
<td>Indicate the following on the identification badge: areas of access (tenant space, utility and mechanical areas, etc.) and purpose of activity on the premises (e.g., organization name, security, maintenance, etc.).</td>
</tr>
<tr>
<td>3.2.04</td>
<td>Identification badges are designed to be easily identifiable (e.g., color, shape, etc.).</td>
</tr>
<tr>
<td>3.2.05</td>
<td>Implement increased security controls (e.g., a PIN [personal identification number], biometric, etc.) to identification badges for access to sensitive or critical areas of the facility. These areas may include: utility connections, loading docks, telecommunications and IT equipment, emergency power supplies, child-care play yards, hazardous-materials storage, HVAC, and other designated critical locations.</td>
</tr>
<tr>
<td>3.2.06</td>
<td>Issue new identification badges to staff or tenants that dramatically change their appearance.</td>
</tr>
<tr>
<td>3.2.07</td>
<td>Personnel identification is worn in a visible location.</td>
</tr>
<tr>
<td>3.2.08</td>
<td>Create and maintain a record of identification badges issued.</td>
</tr>
<tr>
<td>3.2.09</td>
<td>Periodically generate a list of all personnel that have been issued identification badges. Require that all tenants notify security immediately when an employee is fired. Revoke access privileges for fired employees and, if necessary, place them on a Do Not Admit list.</td>
</tr>
<tr>
<td>3.2.10</td>
<td>Visitor log has the following information: name, time, organization visited, and name of person visited and purpose of visit.</td>
</tr>
<tr>
<td>3.2.11</td>
<td>Require requests for temporary and replacement identification badges to be made in writing, particularly the media; persons designated to pick up identification badges must do so in person using photo identification.</td>
</tr>
<tr>
<td>3.2.12</td>
<td>Establish, implement, and maintain procedures for reporting, replacing, and immediately deactivating lost or stolen identification badges. Require departing individuals to surrender their identification badges promptly. Ensure procedures are in place to identify employees that lose their badges.</td>
</tr>
<tr>
<td>3.2.13</td>
<td>Employees are encouraged to question unusual or unrecognized people in or attempting to enter areas where access is restricted.</td>
</tr>
<tr>
<td>3.2.14</td>
<td>Establish through training a security practice where employees do not allow anyone else to enter a controlled area at the same time without using their own credentials; this is often referred to as &quot;piggybacking.&quot; Include instructions to this end in plans and in training sessions.</td>
</tr>
<tr>
<td>3.2.15</td>
<td>As necessary, ensure security guards verify the entrant's identity (e.g., matching face to photo identification). It is preferable that the guard validate the authenticity of the identification presented (e.g., physical inspection of identification).</td>
</tr>
<tr>
<td>3.2.16</td>
<td>Require preclearance of visitors prior to their arrival at the facility.</td>
</tr>
<tr>
<td>3.2.17</td>
<td>Require visitors to sign in and sign out of the site.</td>
</tr>
<tr>
<td>3.2.18</td>
<td>Implement an electronic access tracking system that logs entry into and exit from critical areas.</td>
</tr>
<tr>
<td><strong>3.2.19</strong></td>
<td>Require tenants to pre-register contractors with the site security office. If not pre-registered, confirm the contractor's identity and verify appointment with the tenant prior to granting access.</td>
</tr>
<tr>
<td><strong>3.2.20</strong></td>
<td>Escort is required for all individuals (e.g., visitors, cleaning crews, delivery personnel, maintenance workers, etc.) who do not have the appropriate security clearance to be in sensitive or critical areas. Escorts should be appropriately cleared and remain with the individual.</td>
</tr>
<tr>
<td><strong>3.2.21</strong></td>
<td>Some members of the security staff wear uniforms. Plain clothed security staff are used as appropriate (e.g., to monitor crowded areas). Uniforms should convey professionalism (e.g., slacks, dress shirt, tie (for men), blazer, or in some instances, a business suit). Require uniform vendors to verify the identity of individuals seeking to purchase uniform articles.</td>
</tr>
<tr>
<td><strong>3.2.22</strong></td>
<td>All deliveries are registered with mail room or loading dock; verify registration prior to accepting deliveries. Consider holding courier's identification until delivery is complete.</td>
</tr>
<tr>
<td><strong>3.2.23</strong></td>
<td>Issue and keep a record of parking permits, including identifying information for employee-owned vehicles.</td>
</tr>
<tr>
<td><strong>3.2.24</strong></td>
<td>Vehicle identification information is collected for all vehicles authorized to park on site.</td>
</tr>
<tr>
<td><strong>3.2.25</strong></td>
<td>Enforce use of official parking permits on vehicles using segregated parking areas (e.g., employee, long-term lots). Remove non-registered or illegally parked vehicles.</td>
</tr>
</tbody>
</table>
### 3.3 Information Security

**Scope:** Addresses practices that relate to the protection of sensitive intellectual property kept on site. Excludes cybersecurity.

**Best Practice:** Sensitive information including site security, company, and personnel information is protected from unauthorized access or tampering.

<table>
<thead>
<tr>
<th>Common Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3.3.01</strong></td>
</tr>
<tr>
<td><strong>3.3.02</strong></td>
</tr>
<tr>
<td><strong>3.3.03</strong></td>
</tr>
<tr>
<td><strong>3.3.04</strong></td>
</tr>
<tr>
<td><strong>3.3.05</strong></td>
</tr>
<tr>
<td><strong>3.3.06</strong></td>
</tr>
<tr>
<td><strong>3.3.07</strong></td>
</tr>
<tr>
<td><strong>3.3.08</strong></td>
</tr>
<tr>
<td><strong>3.3.09</strong></td>
</tr>
<tr>
<td><strong>3.3.10</strong></td>
</tr>
<tr>
<td><strong>3.3.11</strong></td>
</tr>
<tr>
<td><strong>3.3.12</strong></td>
</tr>
<tr>
<td><strong>3.3.13</strong></td>
</tr>
<tr>
<td><strong>3.3.14</strong></td>
</tr>
<tr>
<td>3.3.15</td>
</tr>
<tr>
<td>3.3.16</td>
</tr>
</tbody>
</table>
4. Security Systems

### 4.1 Command Center

**Scope:** Addresses practices that relate to the space in which the site security program is managed.

**Best Practice:** A designated space on site is used to manage all aspects of the site security program and supports a common operating picture and situational awareness. Alternatives (locations or technologies) are available in case the primary command center is disrupted or incapacitated by an event.

<table>
<thead>
<tr>
<th>Common Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4.1.01</strong></td>
</tr>
<tr>
<td><strong>4.1.02</strong></td>
</tr>
<tr>
<td><strong>4.1.03</strong></td>
</tr>
<tr>
<td><strong>4.1.04</strong></td>
</tr>
<tr>
<td><strong>4.1.05</strong></td>
</tr>
<tr>
<td><strong>4.1.06</strong></td>
</tr>
</tbody>
</table>
# 4.2 Systems

**Scope:** Addresses the use of human, animal, and technical systems that assist security personnel to detect, monitor, and control terrorist threats.

**Best Practice:** Electronic, physical, canine, or human systems are implemented to deter and mitigate the threat of an act of terrorism and identify site vulnerabilities

## Common Security Practices

### Detecting

| 4.2.01 | Install an intrusion detection system around the envelope of the building and on interior areas, where necessary. Use technologies that are based on the facility's risk assessments. Include glass break sensors on windows up to scalable heights, and a roof intrusion detector. Ensure the intrusion detection system is interoperable with the access control system, CCTV cameras, fire safety system, and other relevant security systems etc. |
| 4.2.02 | Install automatic sprinkler systems to detect and saturate fire that erupts on site. |
| 4.2.03 | Consider using audio analysis to detect suspicious noises (e.g., gunshots and screaming) and to estimate the location of an incident (e.g., shooting, explosion, etc.) through triangulation techniques. Consider the combined use of both video and audio analytics. |
| 4.2.04 | Employ explosive detection canine teams as part of regular or high-visibility patrol teams to detect explosives or other threats. |

### Alerting

| 4.2.05 | Use a multimodal communication system (e.g., mass notification, public address, cell phones, pagers, panic buttons, etc.) that notifies all building occupants of threats and provides emergency instructions. |
| 4.2.06 | Install an alarm system(s) that can verbally advise building occupants of the appropriate action (e.g., evacuate, shelter-in-place) to take in any event. |
| 4.2.07 | Integrate the fire alarm system with other systems (e.g., security, environmental, or building management, etc.) to deliver warnings in tandem or to trigger emergency response during an incident. |
| 4.2.08 | Install duress alarms for employees (e.g., call box, intercom, etc.) in locations (e.g., guard stations, interview rooms, manager or supervisor offices, cash and public transaction areas, site-owned vehicles, or other at-risk areas) where people are vulnerable to attack. Employee duress devices should be enabled for immediate response and concealed from the public. |
| 4.2.09 | Install duress alarms for the general public (e.g., call box, intercom, etc.) in locations (e.g., parking lots, stairwells, waiting rooms, site-owned vehicles, and other at-risk areas) where people are vulnerable to attack. Public duress devices should be enabled for immediate response and highly visible. |
| 4.2.10 | Connect the facility fire alarm system(s) to local emergency services for immediate notification. |
| 4.2.11 | The fire command center includes a public-address system. |

### Screening, Monitoring, and Surveillance (includes visual inspection of people, assets, and places)

<p>| 4.2.12 | Inspect the person and personal items (e.g., briefcases, backpacks, parcels, luggage, etc.) carried by non-identified people (e.g., visitors, contractors, vendors, etc.) before granting entry into the facility. Use one or a combination of the following inspection techniques: visual and hand searches, metal detectors, x-ray scanners, explosive trace detectors, or canines. |
| 4.2.13 | As appropriate, send questionable x-ray images of incoming packages to a remote location where an expert (contractor or vendor) can analyze for detonation material. |
| 4.2.14 | Require adequate security personnel staffing at screening locations to ensure the screening process is performed properly and with an acceptable throughput time. Proper screening may call for one security person to perform only one screening task at a time. |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.15</td>
<td>Establish, implement, and maintain procedures for basic screening of vehicles entering parking areas, with a focus on the driver. At a minimum, inspect the trunk, under the hood, and examine the undercarriage of vehicles that enter facility parking areas. Ensure adequate lighting to illuminate the vehicle exterior and undercarriage. Provide CCTV coverage of the screening area.</td>
</tr>
<tr>
<td>4.2.16</td>
<td>Spot check vehicles at access points or that are parked for long periods of time in or near the facility.</td>
</tr>
<tr>
<td>4.2.17</td>
<td>Move or tow illegally parked vehicles to an appropriate location.</td>
</tr>
<tr>
<td>4.2.18</td>
<td>Monitor designated critical areas (e.g., portals, lobbies, the security command center, utility rooms, loading docks, mail room, parking areas, etc.) in accordance with the facility's risk assessments.</td>
</tr>
<tr>
<td>4.2.19</td>
<td>Monitor intrusion detection systems (cameras), fire, and other alarms, as well as other building systems from a security command center preferably 24-hours a day or in accordance with the facility's risk assessments.</td>
</tr>
<tr>
<td>4.2.20</td>
<td>Use electronic surveillance in locations that provide a view of the building perimeter, specifically activity at primary exits and entrances. Consider using cameras with intelligent video surveillance capability that can automatically identify suspicious activity, abandoned items, unexpected movements, etc. Install cameras at vulnerable access portals. Ensure cameras are interoperable with access control system (i.e., that they respond automatically to interior building alarms and have built-in video motion capability). Use video surveillance equipment that adjusts for environmental conditions (e.g., lighting, distance, vibrations, etc.) and has night vision capability for especially sensitive or critical areas, (e.g., unguarded employee convenience entry doors, rooftops, processing areas, control rooms, communications centers, computer server rooms, shipping areas, mail rooms, fuel or chemical storage tanks, utility access points or service areas, the security operations center, etc.). Interconnect with intrusion, motion, and other detectors (e.g., fire, smoke) as appropriate. Ensure video feeds produce good visual and recording quality. Based on surveillance requirements, assign a sufficient number of security staff to monitor camera feeds. Relieve staff regularly to alleviate fatigue and inattentiveness.</td>
</tr>
<tr>
<td>4.2.21</td>
<td>Monitor site security employees, facility tenants, contractors, delivery personnel, vendors, etc. for suspicious activities (e.g., irregular work hours, attempting to access restricted areas, carrying unusual packages) or behavior.</td>
</tr>
<tr>
<td>4.2.22</td>
<td>Monitor construction work adjacent to the facility (e.g., road construction, utility equipment servicing, etc.) for unusual activities (e.g., placing or planting unusual objects near assets or gathering places).</td>
</tr>
<tr>
<td>4.2.23</td>
<td>Monitor elevator areas designed for both employees and visitors.</td>
</tr>
<tr>
<td>4.2.24</td>
<td>Conduct nonpredictable but recurring, high-visibility patrols to inspect internal and external areas of the facility (e.g., the site perimeter, including fences and gates, parking lots, equipment, sensitive or critical areas, trash and other containers, etc.). Patrols should question suspicious persons and inspect left-behind packages for explosives and other terrorist weapons as set forth in the facility's security policies and plans.</td>
</tr>
<tr>
<td>4.2.25</td>
<td>Use an appropriate number and mix of uniformed and plain clothed security guards to patrol the facility based on the threat level or as determined by risk assessments. For example, increase guard strength during peak hours.</td>
</tr>
<tr>
<td>4.2.26</td>
<td>Establish, if applicable, community policing practices with local law enforcement.</td>
</tr>
<tr>
<td>4.2.27</td>
<td>Enable, if necessary, remote monitoring of the intrusion detection and alarm systems by authorized authorities.</td>
</tr>
</tbody>
</table>

**Access Control - Perimeter**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.28</td>
<td>Protect the facility's perimeter from unauthorized entry as far as practically possible from the building exterior by a physical barrier (i.e., create a buffer zone). Typical perimeter protection barriers include fences, bollards, berms, and concrete walls (Jersey barriers). If necessary, install K12-rated anti-ram bollards around the perimeter of the site or as appropriate.</td>
</tr>
<tr>
<td>4.2.29</td>
<td>Bollards should remain in the up position, except for when they are lowered to allow entry of a screened vehicle.</td>
</tr>
<tr>
<td>4.2.30</td>
<td>For mechanical locks, use a high-security lock and key system with a minimum of six pins. Ensure that the site's key blank is unique. Consult the risk assessment to determine the appropriate extent of the site's access control system.</td>
</tr>
<tr>
<td>4.2.31</td>
<td>Install cameras at critical access portals that trigger an alarm in the command center when a portal is breached.</td>
</tr>
<tr>
<td>4.2.32</td>
<td>Instruct security employees not to hold open or block stairways or fire doors during an emergency. Ensure that the fire command center (a.k.a. fire control room, central control station, fire command station, fire control center) includes a public-address system and allows remote locking or unlocking of stairwells.</td>
</tr>
<tr>
<td>4.2.33</td>
<td>During an active emergency, security controls that restrict egress through exit doors are automatically deactivated (e.g., activation of a fire alarm, sprinkler system, etc.).</td>
</tr>
<tr>
<td>4.2.34</td>
<td>Coordinate access control at the site's perimeter with local law enforcement. Emergency vehicles should have clear access to facility entrances.</td>
</tr>
</tbody>
</table>

**Access Control - Personnel**

| 4.2.35 | Change the password for employee keys and PINS periodically. |
| 4.2.36 | Display identification badge boards and access documentation at access control points or provide security personnel with sheets and cards showing different identification badges where applicable. |
| 4.2.37 | Use security guards (permanent staff or a contract service) to enforce access control. Station access control security guards at main portals and other critical access points in and around the facility. |
| 4.2.38 | When security guards are not present, enforce access control at sensitive locations through mechanical or electronic methods. |
| 4.2.39 | Incorporate screening equipment and procedures (see, “Screening, Monitoring, and Surveillance” under 4.2 Systems), such as magnetometers (metal detectors), x-ray equipment, etc., at main access portals into the access control system. |
| 4.2.40 | The access control system provides an audit trail of ingress into and egress out of the facility and critical areas. Feed real-time audit trail to the facility's command center and main entrance(s) security station to allow for tracking of all site occupants. |
| 4.2.41 | Procedures are in place to identify and admit authorized tenants that cannot present facility access identification badges (i.e., for instances where tenants or employees forget to bring identification badges). |
| 4.2.42 | Limit tenants’ access of facility to public areas and the tenant's own floor(s) through access cards or an appropriate access control method. Ensure that tenants cannot access other tenant space or restricted areas. |
| 4.2.43 | Allow tenants to control access to their floor(s) or areas. |
| 4.2.44 | The property team has plans in place to gain access to tenant areas for emergency purposes. |

**Access Control - Vehicles**

<p>| 4.2.45 | Establish, implement, and maintain a system to control access to parking areas commensurate with the facility's risk assessments and security plans. |
| 4.2.46 | For unattended or high-volume parking areas, use electronic access control methods to control entry and exit (e.g., automated license plate readers, transponders, biometric readers, electronic card readers, or specially issued stickers or placards). |
| 4.2.47 | Install vehicle ingress and egress controls where vehicles and vehicle occupants need to be screened. If necessary, design the vehicular inspection point to include anti-intrusion barriers or vehicle arrest devices that prevent vehicles from leaving the vehicular inspection area and to prevent unauthorized exits. |
| 4.2.48 | Limit vehicular entry and exits to a minimum number of locations, preferably one. |
| 4.2.49 | Remove non-registered or illegally parked vehicles from the premises. |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.50</td>
<td>Park or position facility-owned vehicles to block entrances to and exits from the facilities, when appropriate.</td>
</tr>
<tr>
<td>4.2.51</td>
<td>Access to the facility is controlled from parking areas inside the facility's envelope.</td>
</tr>
<tr>
<td><strong>Utilities and Special Locations</strong></td>
<td></td>
</tr>
<tr>
<td>4.2.52</td>
<td>Control entry to the site during construction so that workers and contractors can only access the parts of the building necessary for construction activities.</td>
</tr>
<tr>
<td>4.2.53</td>
<td>Secure all water supplies at all points of entry into the building.</td>
</tr>
<tr>
<td>4.2.54</td>
<td>Close and lock secondary or nonprimary entrances during evening or off-peak hours.</td>
</tr>
<tr>
<td>4.2.55</td>
<td>Control entry to the site from the loading dock (e.g., use of posted guards, man-trap room, card readers, etc.).</td>
</tr>
<tr>
<td>4.2.56</td>
<td>Use an internal messenger or package delivery system to deliver packages to tenants in lieu of external couriers.</td>
</tr>
<tr>
<td>4.2.57</td>
<td>Secure all utility tunnels, corridors, manholes, storm water run-off culverts, etc., that could give access to the facility. Lock portals to restricted areas (e.g., utility rooms, hazardous material storage areas, voice and data telecommunication system nodes, etc.) and facility control units (e.g., security system panels, fire command center, elevator panels, fuse boxes, etc.), the roof, and any other critical areas or assets. Consider implementing intrusion detection alarms, balanced magnetic contact switches, timed closure devices, etc., to secure access to critical areas and control units. Ensure that on-site or adjacent auxiliary facilities and services (e.g., utility rooms, maintenance closets, etc.) are secure in accordance with site-specific risk and legal regulations.</td>
</tr>
</tbody>
</table>
### 4.3 Redundancy and Diversity

**Scope:** Addresses the use of human and technical systems to ensure the continued accessibility and operation of critical functions before, during, and after an act of terrorism.

**Best Practice:** Where practical, backups or alternatives for critical utilities and security systems are in place to ensure security program functionality during disruptive conditions. Appropriate technologies are employed to facilitate remote or mobile operations of the security program.

<table>
<thead>
<tr>
<th>Common Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.01</td>
</tr>
<tr>
<td>4.3.02</td>
</tr>
<tr>
<td>4.3.03</td>
</tr>
<tr>
<td>4.3.04</td>
</tr>
<tr>
<td>4.3.05</td>
</tr>
<tr>
<td>4.3.06</td>
</tr>
<tr>
<td>4.3.07</td>
</tr>
<tr>
<td>4.3.08</td>
</tr>
<tr>
<td>4.3.09</td>
</tr>
<tr>
<td>4.3.10</td>
</tr>
<tr>
<td>4.3.11</td>
</tr>
<tr>
<td>4.3.12</td>
</tr>
</tbody>
</table>
### 4.4 Maintenance

**Scope:** Addresses policies and procedures used to ensure the continued accessibility and operation of site functions, especially critical functions, before, during, and after an act of terrorism.

**Best Practice:** Security systems and equipment are installed to function properly. They are kept in good working order and they are regularly inspected, calibrated, and otherwise maintained to applicable standards or regulations (national, state, or local). These activities are documented.

<table>
<thead>
<tr>
<th></th>
<th>Common Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4.01</td>
<td>Set in place a service plan, including preventive maintenance schedules, for all facility security and utility systems.</td>
</tr>
<tr>
<td>4.4.02</td>
<td>Prioritize maintenance and repair that could affect the security of facilities such as perimeter fencing, lighting, facility locks, and access points.</td>
</tr>
<tr>
<td>4.4.03</td>
<td>Document regular inspections on all life safety systems, including the fire command center, fire extinguishers, smoke and fire control door systems, automatic sprinkler systems, hose cabinets, stairwell exhaust fans, alarms, elevators and escalators, and emergency exits that demonstrate they are functional. Document progress on addressing any open violations until resolved.</td>
</tr>
<tr>
<td>4.4.04</td>
<td>Perform regular inspection on any chemical, biological, radiation, and nuclear detection or remediation equipment, particularly in the HVAC system, to ensure it is functional.</td>
</tr>
<tr>
<td>4.4.05</td>
<td>Periodically perform maintenance on respiratory protection equipment.</td>
</tr>
<tr>
<td>4.4.06</td>
<td>Have all critical security and utility systems inspected or recommissioned according to industry standards or guidance by qualified personnel following a disruptive incident.</td>
</tr>
<tr>
<td>4.4.07</td>
<td>Calibrate screening equipment according to the manufacturer’s specifications on a regular basis (preferably daily).</td>
</tr>
<tr>
<td>4.4.08</td>
<td>Regularly subject major mechanical, electrical, and plumbing systems to a formal recommissioning process, in accordance with industry standards and guidance.</td>
</tr>
<tr>
<td>4.4.09</td>
<td>Document the location and capacity of major facility systems (e.g., electrical, mechanical, and fire protection, etc.), such as composite drawings, blue prints, etc.</td>
</tr>
<tr>
<td>4.4.10</td>
<td>Maintain, if practicable, in-house staff members to service technological equipment.</td>
</tr>
</tbody>
</table>
5. Communication and Notification

**5.1 Policies and Procedures**

*Scope:* Addresses policies and procedures used to facilitate the site security team’s communication with internal and external stakeholders.

*Best Practice:* Policies and procedures ensure that security information is rapidly and efficiently communicated to and from internal and external stakeholders, including sharing of threats and exchange of information with local, regional, and national sites, organizations, first responders, media, government agencies, and others as necessary. The policies and procedures should be based on the site’s risk assessment and the risk management process.

**Common Security Practices**

<table>
<thead>
<tr>
<th><strong>Internal and Site Operations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5.1.01</strong> Distribute security and emergency response plans to appropriate personnel</td>
</tr>
<tr>
<td><strong>5.1.02</strong> Establish security committees for building management to share security information and engage in regular, structured communication with security staff, tenants, and long-term occupants. Invite, when appropriate, personnel from other properties.</td>
</tr>
<tr>
<td><strong>5.1.03</strong> Set in place a capability for security personnel (guards) to immediately communicate with one another through communication devices (e.g., portable radio, pager, cell phone, personal data assistants [PDAs]).</td>
</tr>
<tr>
<td><strong>5.1.04</strong> Consider adding communication security (e.g., encryption, multiple frequencies) that prevents unauthorized interception of information being transferred.</td>
</tr>
<tr>
<td><strong>5.1.05</strong> Identify the frequencies and channels used by local and state police forces for communications. Coordinate use of appropriate frequencies to ensure communication and deter interference.</td>
</tr>
<tr>
<td><strong>5.1.06</strong> There are redundancies in the communications system that prevent single points of failure (e.g., have backup emergency communication equipment like cell phones or emergency radios available for use in the event that all primary channels are unavailable).</td>
</tr>
<tr>
<td><strong>5.1.07</strong> Alert site occupants immediately to changes in threat level and related changes to security and safety measures. Inform all personnel regularly on the general security situation.</td>
</tr>
<tr>
<td><strong>5.1.08</strong> Issue heightened security awareness alerts, including heightened control measures to vendors and contractors.</td>
</tr>
<tr>
<td><strong>5.1.09</strong> Use more than one medium (e.g., text message, e-mail, phone, etc.) to disseminate general security information to tenants.</td>
</tr>
<tr>
<td><strong>5.1.10</strong> Implement occupant and employee awareness campaigns, such as DHS’s &quot;If You See Something, Say Something.&quot; campaign, for reporting suspicious behavior and activities.</td>
</tr>
<tr>
<td><strong>5.1.11</strong> Establish, implement, and maintain simple, straightforward, and readily available means for personnel to communicate the presence of a threat or an emergency (e.g., panic buttons, hotline number, internal 9-1-1 capability).</td>
</tr>
<tr>
<td><strong>5.1.12</strong> Implement a &quot;dispatcher&quot; system in larger facilities for the security guard communications (radio) network. Design the network to ensure adequate coverage throughout the facility and enable users to contact a security operations center regarding tasks, reporting incidents, and requesting assistance.</td>
</tr>
<tr>
<td><strong>5.1.13</strong> Establish controls to restrict the release of information that might compromise the security posture of the building.</td>
</tr>
<tr>
<td><strong>5.1.14</strong> Instruct employees not to discuss sensitive information over unsecure communication channels.</td>
</tr>
<tr>
<td><strong>5.1.15</strong> In the Security Operations Center, on the designated emergency telephone line, record incoming communications (e.g., 9-1-1 telephone calls) to assist response to requests for assistance or to identify potential threats (e.g. bomb threats).</td>
</tr>
<tr>
<td>5.1.16</td>
</tr>
<tr>
<td>5.1.17</td>
</tr>
<tr>
<td>5.1.18</td>
</tr>
<tr>
<td>5.1.19</td>
</tr>
<tr>
<td>5.1.20</td>
</tr>
<tr>
<td>5.1.21</td>
</tr>
</tbody>
</table>

**Community Partners**

| 5.1.22  | Develop rapport and regularly communicate with appropriate local, state, and federal authorities, public health organizations, industry organizations, and other organizations to enhance information exchange, track threat conditions, report suspicious activity, and support investigations. |
| 5.1.23  | Share and receive security information (e.g., threat advisories and best practices) through local and regional public and private forums. Premise security forums are often hosted by local police and fire departments, industry groups (e.g., the Building Owners and Managers Association [BOMA] International), area security committees, and state and federal agencies. |
| 5.1.24  | Share maps, blueprints, or similar imagery of the physical layout of the facility with appropriate response agencies. Ensure that these maps detail the location of critical assets and relevant site points-of-interest (e.g., water frontage areas, rail lines, emergency access routes, first aid stations, fire hydrants, storage of hazardous material, emergency and utility systems, etc.). |
| 5.1.25  | Institute an "open door" policy for area security staff, authorities, first responders, etc., to visit the site and build rapport with the site's security staff. |
| 5.1.26  | Invite emergency response services to train and run exercises in the facility during off-hours or weekends. |
| 5.1.27  | Use, when practicable and beneficial, the same administrative and training assets (e.g., joint training, joint grant writing, etc.) with appropriate organizations. |
| 5.1.28  | Share external camera feeds with local authorities where available or permissible. |

**Media**

| 5.1.29  | Assign specific employees to interact with the media and to deal with the public in the event of an incident. Ensure that these employees are well versed with site security plans and protocols, participate in all training exercises, and are aware of legal reporting requirements during incidents. |
| 5.1.30  | Establish and use templates for press releases and written communication to the public. Ensure that all templates are pre-approved by site legal counsel. |
### 5.2 Signage and Announcements

**Scope:** Addresses policies and procedures related to the use of communication aids by the site security team before, during, and after an act of terrorism.

**Best Practice:** Clear, simple communication (e.g., physical signs, public address announcements, and other notification techniques) is made to internal or external stakeholders on site security information, policies, and procedures in accordance with applicable regulations, codes, and the site security program.

<table>
<thead>
<tr>
<th>Common Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5.2.01</strong></td>
</tr>
<tr>
<td><strong>5.2.02</strong></td>
</tr>
<tr>
<td><strong>5.2.03</strong></td>
</tr>
<tr>
<td><strong>5.2.04</strong></td>
</tr>
<tr>
<td><strong>5.2.05</strong></td>
</tr>
<tr>
<td><strong>5.2.06</strong></td>
</tr>
<tr>
<td><strong>5.2.07</strong></td>
</tr>
<tr>
<td><strong>5.2.08</strong></td>
</tr>
</tbody>
</table>
### 6. Defensible Space Design

#### 6.1 Physical Structure

**Scope:** Addresses policies and procedures related to the design, construction, operation, and retrofitting of all structures and related exterior infrastructure, as well as interior technical systems, covered by the site security program.

**Best Practice:** The physical structure of the site and security systems are designed and hardened to meet or exceed the risks identified for the facility and the requirements (state and local codes and regulations) in place at the time of original construction. New facilities, new additions, and areas undergoing major renovations meet or exceed the risks identified at the time of new construction and comply with current codes and regulations. A CPTED approach is used for space design. Physical protections add structural resilience and secure and enhance security systems on an ad hoc basis, as the need arises.

<table>
<thead>
<tr>
<th>Common Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.01 Design the building to promote a sense of implemented security measures, the presence of security staff, reduced areas of concealment, continuous monitoring, controlled access and appropriate responsive measures. Example proofs of intent include plans, elevations and photographs showing clear lines of sight for security stations, eliminated blind corners, appropriate illumination, maximized security visibility, natural barriers, separation of protected spaces, etc.</td>
</tr>
<tr>
<td>6.1.02 Glass should be selected and designed in accordance with relevant standards to meet the security requirements of the threat(s), threat locations and vulnerabilities identified in the site risk assessment.</td>
</tr>
<tr>
<td>6.1.03 Glass in high-risk areas is designed in accordance with relevant standards and to meet the security requirements of the threat(s), threat locations and vulnerabilities of the risk assessment. Reference: American Society for Testing and Materials (ASTM) F 1642-12 (current version) &quot;Standard Test Method for Glazing and Glazing Systems Subject to Air Blast Loadings.&quot;</td>
</tr>
<tr>
<td>6.1.04 Refuge or shelter in place areas should be designed in the facility. These areas should be well protected through use of location, appropriate enclosure and security systems.</td>
</tr>
<tr>
<td>6.1.05 Minimize egress between residential areas and nonresidential areas if the site is mixed-use. Seal off all residential areas from all restricted areas without compromising the facility's fire life safety practices.</td>
</tr>
<tr>
<td>6.1.06 For high ceiling heights (over 16 feet), discontinuous columns, long spans and other potential structural deficiencies conduct and document a thorough structural review.</td>
</tr>
<tr>
<td>6.1.07 Areas containing critical assets should be protected through effective location, and appropriate enclosure and security systems.</td>
</tr>
</tbody>
</table>

**Reinforcement/Protection**

| 6.1.08 Design the building enclosure and structure to withstand blast loads and progressive collapse related to identified threats from the site risk assessment. Current building code natural hazards loadings should be documented, and additional blast loads calculated and designed into the building. Example proofs of level of protection provided that should be available for inspection include structural calculations and analysis of blast loading for the enclosure and structural systems, and progressive collapse evaluation for the building structural system. |
| 6.1.09 Mark front and rear facility doors with the facility's address, on or above the doors. Peepholes should be designed into exterior doors to enhance surveillance of the facility's exterior. |
| 6.1.10 Securely anchor exterior doors to a structure using a metal frame that is grouted with cement. |
| 6.1.11 Mount exterior doors to ensure that they open outward—that is, away from an interior space. |
| 6.1.12 Install hinges on the door interior to prevent removal of exterior doors from the hinge side, provide concealed hinges, and use heavy-duty grade with nonremovable pins. If removable pins are installed, weld them in place to prevent their removal and reduce their vulnerability to tampering. |
| 6.1.13 | Use industry standard ballistic level protection rating to specify unglazed exterior doors that require ballistic-level protection. |
| 6.1.14 | Ensure high-risk-area doors use ballistic protections against adversary actions to penetrate the opening. |
| 6.1.15 | Install interior glass that is shatter-resistant (e.g., the glass is glazed or is fully tempered safety glass that can withstand a pressure of 16,000 psi). |
| 6.1.16 | Secure nonwindow openings greater than 96 square inches in perimeter walls with grilles, bars, or alarms. |
| 6.1.17 | Mount overhead objects (light fixtures, etc.) weighing 31 pounds (14 kilograms) or more using either a rigid or flexible system to minimize likelihood of falling. Suggested mounting systems will resist a downward force of 1.5 times the weight of the object and 0.5 the object's weight in a horizontal direction. |
| 6.1.18 | Secure ladders, awnings, and parapets that give access to building roofs, HVAC systems, and other critical equipment. Limit and trim nearby foliage (e.g., trees, shrubs) so it cannot be used to gain access to the roof. |
| 6.1.19 | Doors and walls along the line of security screening meet requirements of UL 752 "Standard for Safety: Bullet-Resisting Equipment." |
| 6.1.20 | Secure incoming communication equipment (telephone, Internet, etc.) from external tampering by placing transformers or switchgears where they are not accessible from outside the building. |
| 6.1.21 | Harden enclosures and pathways for emergency egress to limit the extent of debris that might impede safe passage and reduce the flow of evacuees. |
| 6.1.22 | Fenestration glass, particularly to scalable heights, should be suitably protected (e.g., by glazing) against impact and shattering into shards, per the facility's risk assessment. |
| 6.1.23 | Cameras have housings designed to protect them against exposure or tampering. |
## 6.2 Protected Areas

**Scope:** Addresses policies and procedures related to the design, construction, operation, and retrofitting of all public spaces, including interior spaces, covered by the site security program.

**Best Practice:** Based on the identified risk, areas open to the public where access is monitored, limited, or controlled are designed and located to enhance detection and apprehension of illicit activity as well as to mitigate consequences from an act of terrorism.

### Common Security Practices

#### Portals (entry and exit)

| 6.2.01 | Locate, if site allows, pedestrian access control and inspection points at the perimeter of the site, as far from the facility as possible. |
| 6.2.02 | Locate vehicle access control and inspection points at the perimeter of the site, as far from the facility as possible. |
| 6.2.03 | Locate guard stations and kiosks so that site staff and security officers have optimum sight lines into and out of portal areas. |
| 6.2.04 | Use single- or double-leaf configurations and commercial security hollow metal exterior doors (exterior doors) as the facility's general public entrance and exit doors or as service entrances for facility operations personnel. |
| 6.2.05 | Limit the number of exterior doors to reduce the number of vulnerabilities to the facility's envelope. |
| 6.2.06 | Install automatic door closers and locks on the outside of exterior doors other than the main lobby entrance. Automatic locks must not restrict evacuation during emergency conditions. |

#### Lobby, Concourse, and Waiting Areas

| 6.2.07 | Conduct visitor screening where site configuration allows in an area outside the main building footprint to prevent incidents in the lobby from impacting the rest of the facility. |
| 6.2.08 | If possible, design the lobby or waiting areas to increase throughput (reduce queuing) while maintaining the effectiveness of the security measures. Reduce queuing time in these areas by maximizing the number of visitor receptionists, screening lanes, and the processing speed of access control systems. |
| 6.2.09 | Minimize public restrooms in nonsecure areas. Locate public restrooms away from the main facility entries and exits. |

#### Stairwells

| 6.2.10 | Locate stairways for emergency egress as remote as possible from high-risk areas, and design them to discharge into areas other than lobbies, parking zones, or loading docks. |
| 6.2.11 | Use different stairwells for evacuation and for "attack" by first responders, install fire hose connectivity in "attack" stairwell(s), and use double-wide stairwells for "evacuation" stairwell(s). |
| 6.2.12 | Eliminate potential hiding places (nooks and crannies) below stairways. |

#### Elevators

| 6.2.13 | Install CCTV in all freight elevators. If necessary, install cameras in public elevators. |
| 6.2.14 | Install an emergency message capability on elevators. |

#### Parking

| 6.2.15 | Design, as site configuration allows, parking areas adjacent to or as far from the facility and critical assets as practicable. Limit parking areas inside the facility's envelope. |
| 6.2.16 | Locate vehicle access control and inspection points at the perimeter of the site as far from the facilities as possible. |
| 6.2.17 | Establish and enforce a minimum setback and standoff distance between the facility envelope and parked vehicles. (For guidance, consult the DHS Science and Technology's Building and Infrastructure Protection Series [BIPS] publication BIPS-06 "Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings."
| 6.2.18 | Parking garages and parking lots should be located and designed to present the lowest number of vulnerabilities to the building and occupants. |
| 6.2.19 | There is adequate visibility (line-of-sight or cameras) across, into, and out of parking lots and garages. |
| 6.2.20 | Separate visitor parking from occupant parking. |
| 6.2.21 | Establish controls so that vehicles are not left unattended in driving lanes that are closer to the buildings than the required standoff distance set for the facility. |
| 6.2.22 | Design stair and elevator waiting areas of parking structures such that they are visible to the exterior and keep parking areas well lit. |
| 6.2.23 | Control curb-lane parking such that unauthorized vehicles are not allowed to park close to a building. |
| 6.2.24 | Allow no dead-end parking areas in parking lots that are within the standoff distances set for the facility. |

**Vehicle/Pedestrian Channels**

| 6.2.25 | Design traffic patterns to ensure circulation that prevents high-speed approaches by visitors; barriers, planters, and landscaping may be useful. |
| 6.2.26 | Provide an interior perimeter road for patrols where the perimeter barrier (e.g., fencing) encloses an area generally greater than 1 square mile (2.6 km2). Drainage culverts passing under the road in clear zones must be secured at all openings for drainage and culverts under fences. |
| 6.2.27 | Perform periodic maintenance of the perimeter roadway to prevent or remove overgrown vegetation, trees, or shrubs, ensure snow or other debris removal, maintain an unobstructed line of sight along the property boundary, and prevent damage to vehicles using the road. |

**Lawns and Grounds**

| 6.2.28 | Install landscaping to be a physical barrier for the building and obstruct view angles (take care not to create hiding places), but not to obstruct the lines of sight to see pedestrians or vehicles approaching the building. |
| 6.2.29 | Utilize landscaping and other site features to provide for effective surveillance and reduce opportunities for concealment or entry into the facility. |

**Restrooms**

| 6.2.30 | Publicly accessible restrooms are key locked and use a key control system. If there is a combination lock, only authorized personnel should open the lock for visitors. |

**Miscellaneous Areas**

| 6.2.31 | Protect and secure onsite or adjacent auxiliary facilities and services (e.g., day care center) consistent with the security plan. |
### 6.3 Controlled and Restricted Areas

**Scope:** Addresses policies and procedures related to the design, construction, operation, and retrofitting of all nonpublic spaces covered by the site security program.

**Best Practice:** Based on the identified risk, areas on the premises where access is strictly or tightly controlled are designed and located to enhance detection and apprehension of illicit activity as well as to mitigate consequences from an act of terrorism.

#### Common Security Practices

<table>
<thead>
<tr>
<th><strong>Roof</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.3.01</strong></td>
</tr>
<tr>
<td><strong>6.3.02</strong></td>
</tr>
<tr>
<td><strong>6.3.03</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Storage</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.3.04</strong></td>
</tr>
<tr>
<td><strong>6.3.05</strong></td>
</tr>
<tr>
<td><strong>6.3.06</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Mail Room</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.3.07</strong></td>
</tr>
<tr>
<td><strong>6.3.08</strong></td>
</tr>
<tr>
<td><strong>6.3.09</strong></td>
</tr>
<tr>
<td><strong>6.3.10</strong></td>
</tr>
<tr>
<td><strong>6.3.11</strong></td>
</tr>
<tr>
<td><strong>6.3.12</strong></td>
</tr>
<tr>
<td><strong>6.3.13</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Loading Dock</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.3.14</strong></td>
</tr>
<tr>
<td><strong>6.3.15</strong></td>
</tr>
<tr>
<td><strong>6.3.16</strong></td>
</tr>
<tr>
<td><strong>6.3.17</strong></td>
</tr>
</tbody>
</table>
### 6.4 Accessories

**Scope:** Addresses policies and procedures related to the design, construction, operation, and retrofitting of all interior fixtures and other accessories (excluding security systems) covered by the site security program.

**Best Practice:** Based on the identified risk, site accessories (e.g., trash cans, vending machines, water fountains, mailboxes, aesthetics, newspaper stands, bike racks, etc.) are designed and located to reduce the risk of the object being used as a terrorist tool as well as to mitigate consequences from an act of terrorism.

<table>
<thead>
<tr>
<th>Common Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.4.01</strong></td>
</tr>
<tr>
<td><strong>6.4.02</strong></td>
</tr>
<tr>
<td><strong>6.4.03</strong></td>
</tr>
<tr>
<td><strong>6.4.04</strong></td>
</tr>
<tr>
<td><strong>6.4.05</strong></td>
</tr>
<tr>
<td><strong>6.4.06</strong></td>
</tr>
<tr>
<td><strong>6.4.07</strong></td>
</tr>
<tr>
<td><strong>6.4.08</strong></td>
</tr>
<tr>
<td><strong>6.4.09</strong></td>
</tr>
</tbody>
</table>
### 6.5 Utility Systems and Equipment

**Scope:** Addresses policies and procedures related to the design, construction, operation, and retrofitting of all exterior and interior utility systems covered by the site security program.

**Best Practice:** Based on the identified risk and assessment of the cost-benefit, utility systems (HVAC, electrical, etc.) are designed and located to reduce the risk of their use as a terrorist tool as well as to mitigate consequences from an act of terrorism.

#### Common Security Practices

| 6.5.01 | Consider the security of the physical location of critical assets when planning and performing new construction or major renovations. |
| 6.5.02 | Place critical assets (safes, fuel supplies, computer servers, HVAC system, fire life safety control system, command center, etc.) in secure areas away from vulnerable areas, such as portals, vehicle circulation areas, areas of congestion, parking, maintenance areas, loading docks, or utility systems. |
| 6.5.03 | Locate redundant and backup equipment in a different part of the building than primary equipment. |
| 6.5.04 | Locate utility supply facilities and equipment that are potentially hazardous (e.g., liquid fuel tanks, high-voltage power lines) at a safe distance from the building or in areas where large numbers of people congregate. Locate these supplies off-site, if possible. |
| 6.5.05 | Protect nonwindow openings, such as mechanical vents and exposed plenums so that they provide the same level of protection required for the exterior wall. Install lighting around the facility's perimeter. |

#### Air Supply

| 6.5.06 | Locate fresh air intakes on the fourth floor or as high as practical (fifty feet above ground is recommended). Location on a wall is preferred over a roof. |
| 6.5.07 | Design fresh air intakes so that debris rolls off (e.g., cover openings with screens or slope them downward). |
| 6.5.08 | The HVAC system can sustain other systems (e.g., servers, fire command center, etc.) that require temperature and humidity control. |
| 6.5.09 | HVAC and the exhaust system are designed for rapid shutdown. |
| 6.5.10 | Establish HVAC zones for lobbies, mail rooms, loading docks, and other entry and storage areas that can maintain negative pressure to contain releases of CBRN materials. |
| 6.5.11 | Air intakes and exhausts are closed when not operational. |
| 6.5.12 | Install air monitors or sensors for CBRN agents in the air handling system. |
| 6.5.13 | Filter HVAC exterior air handling units using, for example, high efficiency particulate arrester (HEPA) filters. |
| 6.5.14 | Install, to the extent possible, multiple air intake locations. |

#### Electrical Supply and Telecommunications

| 6.5.15 | Install more than one entry point for electrical service to the facility. |
| 6.5.16 | Use ducts and other conduits to run utility service through the facility. |
| 6.5.17 | Install redundant nodes in the electrical system such that if a node is disrupted, it would not eliminate both normal electrical service and emergency backup power. |
| 6.5.18 | Have electrical service provided from at least two different sources (i.e., substations) where possible. |
| 6.5.19 | Have in place two minimum-points-of-presences (MPOPs) for communication equipment. |
7. Performance Evaluation

### 7.1 Exercising and Testing

**Scope:** Addresses policies and procedures related to the exercise of all functions under the site security program, as well as the testing of related equipment and systems to ensure proper functionality.

**Best Practice:** Security plans and procedures are regularly practiced or exercised to ensure that they function in accordance with security program objectives and the Homeland Security Exercises and Evaluation Program (HSEEP). When possible, exercises incorporate all tenants and responding agencies, and address issues of unified command and control. Security systems and equipment are regularly tested to assure they function as intended. Exercise and testing activities are documented.

#### Common Security Practices

<table>
<thead>
<tr>
<th>Group</th>
<th>7.1.01</th>
<th>7.1.02</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td>Instill a security culture of periodically exercising all security related plans, procedures, and products.</td>
<td>Document the dates and outcomes of all exercises or tests of security plans, procedures, and products.</td>
</tr>
</tbody>
</table>

#### Exercising

<table>
<thead>
<tr>
<th>7.1.03</th>
<th>Regularly exercise property team and security staff on aspects of site security plans.</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1.04</td>
<td>Exercise the communication and notification plan. Ensure a simple and straightforward means for people to send and receive information regarding a potential threat or an emergency.</td>
</tr>
<tr>
<td>7.1.05</td>
<td>Exercise facility emergency procedures periodically with building occupants. Vary exercises to test all types of foreseeable incidents. Evaluate all exercises and immediately inform appropriate personnel and all site occupants of any changes.</td>
</tr>
<tr>
<td>7.1.06</td>
<td>Invite neighboring buildings to participate in emergency drills and training exercises to extend knowledge and outreach should emergencies occur.</td>
</tr>
<tr>
<td>7.1.07</td>
<td>Invite local law enforcement and emergency responders to participate in emergency drills and training exercises to familiarize them with the building and its security and emergency procedures.</td>
</tr>
</tbody>
</table>

#### Testing

<table>
<thead>
<tr>
<th>7.1.08</th>
<th>Test periodically all access control devices (e.g., electronic readers) to be sure they are providing timely and accurate (proper identity verification) access.</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1.09</td>
<td>Test periodically all video equipment to ensure clear lines-of-sight and to ensure they otherwise proper functionality, including the ability to record and time and date stamps.</td>
</tr>
<tr>
<td>7.1.10</td>
<td>Test periodically all emergency response equipment according to manufacturer instructions.</td>
</tr>
<tr>
<td>7.1.11</td>
<td>Test periodically all life safety systems, including fire extinguishers, alarms, elevators and escalators, and emergency exits to ensure functionality. Ensure that lighting along evacuation paths is functional when normal power is interrupted.</td>
</tr>
<tr>
<td>7.1.12</td>
<td>Test periodically all contact databases, calling trees, notification and recall lists, and other communications lists.</td>
</tr>
</tbody>
</table>
### 7.2 Evaluation

**Scope:** Addresses policies and procedures related to the formal and informal assessment and improvement of all exercises, tests, and incidents related to the site security program.

**Best Practice:** Security program procedures and capabilities are evaluated for suitability, adequacy, and effectiveness through periodic reviews, post-incident reporting, and performance evaluations, applying metrics where relevant. The method of evaluation is in accordance with the Homeland Security Exercises and Evaluation Program (HSEEP). This responsibility is assigned by top management to an individual and conducted without influence of top management. Evaluations are used to inform and make recommendations to top management regarding the status of the security program, appropriate corrective actions, and opportunities for continuous improvements. An internal audit of the security program is conducted by a qualified individual periodically, typically annually. This audit is conducted free of top management influence and is independent of other evaluation activities.

#### Common Security Practices

| 7.2.01 | Conduct security program audits at least annually. Ensure a security review committee (or other designated group) addresses the findings and recommendations from audits, and updates plans, protocols, and processes as necessary. |
| 7.2.02 | Have local law enforcement or a qualified third-party vendor perform a security audit of the building. |
| 7.2.03 | Develop site-specific performance measures that measure the effectiveness of the security program. Compare current performance to past performance. Examples include: degree of a security activity's implementation; the number of risk assessments completed during a calendar year; determining the security program's effect on risk over time; documenting and analyzing the frequency and impact of security-related incidents over time; and the number of access control failures. |
| 7.2.04 | Where possible, conduct comparisons of performance measures with external properties. |
| 7.2.05 | Establish a self-assessment competency to provide internal audits of program implementation and outcomes. |
| 7.2.06 | Document all incidents that occur at the site or are relevant to the site's security environment. |
| 7.2.07 | Evaluate periodically incident reports to determine if changes in site security policy, procedure, or practice are needed. |
| 7.2.08 | Prepare after action reports on emergency drills and exercises. Use these reports to inform improvements to the security system and as documentation that the exercise was conducted. |
| 7.2.10 | Review and evaluate the recovery plan periodically (e.g., through table-top exercises, etc.). Invite appropriate external stakeholders to participate. |
Guide: Conducting BPATS Based Assessments of Commercial Facilities

Field Guide: Conducting BPATS Based Assessments of Commercial Facilities

(BPATS - Best Practices for Anti-Terrorism Security)

BPATS 1.1 Top Management Commitment
BPATS Assessment Tool Flowchart
BPATS Assessment Tool Input Screen

August 2018
The BPATS Assessment Tool (the "Tool") was developed by the National Institute of Building Sciences (Institute) under contract to the United States Department of Homeland Security (DHS), Science and Technology Directorate, Office of the SAFETY Act Implementation (OSAI). Both the Institute and the United States Government own and hold property rights and interests in and to the Tool and reserve all such rights therein. You are hereby permitted to use the Tool for its intended purpose of assessing the security features, practices and procedures of your commercial facility. Use of the Tool for purposes for which it is not intended is hereby prohibited. You may not reproduce and publish or otherwise distribute or display the Tool to others for commercial or other unauthorized purposes. You may not modify the Tool or create derivative works based on the Tool without express written approval of both the Institute and the DHS OSAI.

DISCLAIMER: NEITHER THE INSTITUTE, THE DHS, NOR THE UNITED STATES GOVERNMENT WARRANTS OR GUARANTEES THAT USE OF THE BPATS ASSESSMENT TOOL WILL PROTECT USER, USER'S FACILITY, OR PERSONS OCCUPYING USER'S FACILITY FROM HARM, INJURY, LOSS OR DAMAGES CAUSED BY TERRORIST OR OTHER CRIMINAL ACT DIRECTED AGAINST THE FACILITY OR ITS OCCUPANTS. NEITHER THE INSTITUTE NOR THE UNITED STATES GOVERNMENT, OR ANY AGENCY OR DEPARTMENT THEREOF, ASSUMES ANY LIABILITY WHATSOEVER FOR INJURY, LOSS OR DAMAGES INCURRED BY A FACILITY OR ANY PERSON(S) OCCUPYING A FACILITY BASED UPON OR ALLEGED TO BE BASED UPON USE OF THIS BPATS ASSESSMENT TOOL FOR COMMERCIAL FACILITIES.
Field Guide: Conducting BPATS Based Assessments of Commercial Facilities

Acknowledgments

The Office of SAFETY Act Implementation, Science and Technology Directorate, Department of Homeland Security (DHS) acknowledges the assistance of the National Institute of Building Sciences in the development of this Field Guide and revising and expanding the original Best Practices for Anti-Terrorism Security and the process identified in the “The Manual for Assessors for Anti-Terrorism Facility Security Systems Metropolitan Commercial Office Buildings, DHS, Pre-Decisional 2015.” on which this Field Guide is based.

The Office of SAFETY Act Implementation also acknowledges Homeland Security Studies and Analysis Institute (HSSAI) for compiling the original Best Practices for Anti-Terrorism Security and developing the original manual. HSSAI is a Federally Funded Research and Development Center established for the DHS.

Project Officer

Bruce Davidson, Department of Homeland Security (DHS), Science and Technology Directorate, Office of the SAFETY Act Implementation (OSAI)

Project Managers

Leya Posey, Department of Homeland Security (DHS), Science and Technology Directorate, Office of the SAFETY Act Implementation (OSAI)

Roger Grant, National Institute of Building Sciences

Author

Terrence Ryan, TRyan AT FP, LLC

Software Developer

Bob Payne, National Institute of Building Sciences

Contributors

Earle Kennett, National Institute of Building Sciences
# Table of Contents

Acknowledgments ........................................................................................................................................... i

1. Introduction .................................................................................................................................................. 1

2. Overview ..................................................................................................................................................... 1

3. Key Assessment Concepts ......................................................................................................................... 1

4. Assessment Scope ...................................................................................................................................... 2

5. Assessment Process .................................................................................................................................... 2

5.1. Documentation Review .......................................................................................................................... 2

5.1.1. Document Review List ......................................................................................................................... 3

5.1.2. Document Rating Scale ......................................................................................................................... 4

5.2. Site Visit ................................................................................................................................................... 5

5.2.1. Site Visit Plan .......................................................................................................................................... 5

5.2.2. Assets, Functions, Infrastructure ........................................................................................................... 5

5.2.3. Tour Checklist ......................................................................................................................................... 6

5.2.4. Threats .................................................................................................................................................... 7

5.2.5. Comparison analysis to Best Practices for Anti-Terrorism Security (BPATS) ........................................ 8

5.2.6. Best Practices for Anti-Terrorism Security (BPATS) Ratings ............................................................... 10

5.3. Report Development ............................................................................................................................... 11

5.3.1. Assessment Team .................................................................................................................................. 12

5.3.2. Executive Summary ............................................................................................................................. 12

5.3.3. Assessment Worksheets ...................................................................................................................... 12

5.3.4. Lessons Learned .................................................................................................................................... 13

5.3.5. Routing of Reports ............................................................................................................................. 13

6. Owner/Operator Actions ............................................................................................................................ 14

6.1. Post Assessment Actions: Mitigation, Deferred Mitigation, Acceptance of Risk .................................. 14

6.2. Recording Post Assessment Actions in the BPATS Tool ........................................................................ 15

6.3. Samples of Owner Comments to include operational procedures and technology ............................. 16
1. Introduction
The Department of Homeland Security (DHS) has national leadership responsibilities for managing risks involving critical infrastructure, key resources, and events. DHS has identified commercial facilities as key assets in the critical infrastructure/ key resource sector and encourages the widespread deployment of effective anti-terrorism technologies, services and capabilities. Building security programs are a technology that may receive Designation under the SAFETY Act.

To help commercial building owners and managers, the Science and Technology Directorate, Office of SAFETY Act Implementation identified a set of best operational security practices for metropolitan commercial office buildings, referred to as Best Practices for Anti-Terrorism Security or BPATS. This list is available to owners and assessors in this Field Guide. There was also a need for an assessment methodology that could be used to record and compare a facility’s practices to the BPATS. This Field Guide and the associated online tool meets that need by providing a recommended process that can be used to improve the content and persuasiveness of assessments.

2. Overview
The guide starts with the key concepts of a BPATS based assessment and then provides information on the three-phase assessment process: The Documentation Review phase, the Site Visit phase, and the Report Development phase. The guide finishes with a review of Owner / Operator post assessment actions. Appendix A of the Guide contains the BPATS list. Seven practice categories are used to organize the 24 BPATS. There are 411 Common Security Practices in the 24 BPATS and the determination of the extent to which the Building Security program incorporates each of these BPATS’ is a key part of the assessment.

3. Key Assessment Concepts
As we go through the process, there are several key concepts to remember.

- First, this is an assessment process using best practices for anti-terrorism security, or BPATS, not for all hazards. Vulnerabilities to other threats, such as earthquakes, floods or other natural hazards, may not be discovered through this process.
- The assessment is not a pass / fail process; it is the description of a snapshot in time of a building’s security program. Few, if any, security programs will meet all best practices.
- Assessments should identify notable strengths as well as areas that may need further development.
- When performing an assessment think beyond a “conformity assessment” and ask, “is the system effective in facilitating the defense against acts of terrorism?” Use the list of BPATS to organize the report, but not to limit the findings and assessment.
- Whatever the findings are to the best practice comparison, remember they need to be evidence based. For example, they should state written policy evidence, plus records or incident report evidence to support the finding.
• Assessment reports must include a clear statement of scope of the assessment and define any assumptions and limitations. For example: the scope could be the security program for just a project’s high-rise, or the high-rise and a plaza, or the high-rise, plaza and the parking garage.

• The BPATS-based assessment covers physical methods of attack to personnel and tangible property, with an emphasis on terrorism. Methods of attack may be split into two broad categories: physical threats to personnel and tangible property, and threats of electronic or computer-based attacks on the information systems. The BPATS based assessment described in this guide only covers the physical methods of attack, not computer-based attacks on the information systems. For cyber threats, there are other cyber assessment tools like the CSET (Cyber Security Evaluation Tool). Please note however, there is a section on “Information Security” included in the BPATS, which addresses the physical protections of IT systems.

4. Assessment Scope
Before starting an assessment, confirm the assessment’s scope. An assessment scope statement is an essential element of any project. It is a tool used to describe the major deliverables of a project including the key milestones, high level requirements, assumptions, and constraints. It also defines the boundaries of a given project and clarifies what deliverables are in and out of scope.

Note: If the Assessment report is included as part of a SAFETY Act Application, the assessment scope statement will be compared to the SAFETY Act Application Technology Description.

5. Assessment Process
The BPATS based assessment process consists of three steps:

• Step 1: Review documentation to determine if facility management has properly established, implemented, and maintained an anti-terrorism security program
• Step 2: Visit the site to visually establish that the security system functions and infrastructure are in place and operational
• Step 3: Complete an assessment report that documents findings. These findings should be detailed and should be based in evidence found in steps 1 and 2.

More than one assessor may conduct the assessment. For example, a Physical Security Subject Matter Expert (SME) and a Building Systems SME may form a team and divide the work appropriately.

Before any work is done, assessors should expect to establish a non-disclosure agreement (NDA) with the owner / manager. The NDA may help with information exchange and information in the NDA is listed as a part of the final report.

5.1. Documentation Review
Documentation review is the first step in the assessment process. Documentation provides evidence about how a building’s security program has been established, implemented and maintained. This review may be done prior to the site visit if you are allowed access to documents, or if documents are not released, it may be done during the first part of the on-site assessment. Items to review include management documents, such as staffing, organization and budgeting guidance; plans such as the
emergency action plan, the continuity of operations plan and the tenant handbook; reports and studies such as an engineering analysis on blast; as well as facility and security force policies and procedures.

First, conduct a brief review to make sure the site has enough information to conduct a security review with respect to the BPATS. As needed, request missing information from the facility. If there is not enough documentation, you should delay the assessment until the necessary documentation is available.

Next, determine how each document or record provides or does not provide adequate evidence of a Best Practice - think of this as a two or three-point verification with a clear record of recent actions or events. For example, there should be a security plan plus a record of quarterly meetings reviewing the program; a written security procedure plus an after-action report from the latest incident response; and a security system layout and design concept, in addition to records of quarterly tests, repairs and maintenance.

Finally, cross check the documents to ensure the policies and procedures correlate. For example, the same list of hazards in the Continuity of Operations plan should also be addressed in the Tenant Handbook and in the Security Force Procedures.

5.1.1. Document Review List

The document list is a mixture of items: some are evidence of a best practice and some facilitate and support the assessment. For example:

- Floor plans facilitate site tours and understanding the buildings layout and design
- Exercise After Action Reports are evidence how the building’s security program is being testing and improved

Recommended documentation to review is listed in the table below. Next to each document is a reference to the corresponding BPATS or a note that the document is a facilitating and supporting item. In addition to the types of documentation listed, you may consider any other types of documents and records relevant to the assessment scope. (See TABLE 1: DOCUMENTATION REVIEW LIST)

<table>
<thead>
<tr>
<th>Document</th>
<th>BPATS Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building Plans and Elevations</td>
<td>(facilitating and supporting item)</td>
</tr>
<tr>
<td>Building Interior Diagrams and Layouts</td>
<td>(facilitating and supporting item)</td>
</tr>
<tr>
<td>Incident Response Plans</td>
<td>2.3 Incident Preparedness, 2.4 Incident Response and Recovery</td>
</tr>
<tr>
<td>Security Policies (Building Occupants)</td>
<td>1.1 Top Management Commitment, 1.2 Policy, 2.2 Risk Awareness, 3.3 Information Security</td>
</tr>
<tr>
<td>Security Staff Procedures (i.e. Post Orders)</td>
<td>2.1 Risk Assessment, 2.3 Incident Preparedness, 2.4 Incident Response and Recovery, 2.5 Continuity of Operations, 3.1 People Surety, 3.2 Identification and Verification, 3.3 Information Security, 4.2 Systems, 5.1 Policies and Procedures, 6.3 Controlled and Restricted Areas</td>
</tr>
<tr>
<td>Document</td>
<td>BPATS Reference</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Continuity of Operations Planning</strong></td>
<td>2.1 Risk Assessment, 2.3 Incident Preparedness, 2.5 Continuity of Operations</td>
</tr>
<tr>
<td><strong>Training Records of the Security Staff</strong></td>
<td>3.1 People Surety</td>
</tr>
<tr>
<td><strong>Incident Reports</strong></td>
<td>2.1 Risk Assessment, 7.2 Evaluation</td>
</tr>
<tr>
<td><strong>Life Safety System Inspection Reports including Open Violation Progress Reports</strong></td>
<td>(facilitating and supporting item)</td>
</tr>
<tr>
<td><strong>Risk Assessments and Threat Assessments</strong></td>
<td>1.2 Policy, 1.3 Scope and Objectives, 2.1 Risk Assessment, 2.3 Incident Preparedness, 3.3 Information Security, 5.1 Policies and Procedures, 7.2 Evaluation</td>
</tr>
<tr>
<td><strong>Building Construction Specifications</strong></td>
<td>(facilitating and supporting item)</td>
</tr>
<tr>
<td><strong>Plans depicting the location of fire, camera and security systems</strong></td>
<td>(facilitating and supporting item)</td>
</tr>
<tr>
<td><strong>Security Program Audit Reports</strong></td>
<td>7.2 Evaluation</td>
</tr>
<tr>
<td><strong>Security tests or table top exercise records</strong></td>
<td>2.4 Incident Response and Recovery, 3.3 Information Security, 7.1 Exercising and Testing, 7.2 Evaluation</td>
</tr>
<tr>
<td><strong>Diagram listing the location of technology assets controlled by building management such as electronic mail or web servers, data centers, networking nodes, controlled interface equipment and communications equipment</strong></td>
<td>(facilitating and supporting item)</td>
</tr>
<tr>
<td><strong>Engineering Analysis on Blast Protection</strong></td>
<td>6.1 Physical Structure, 6.3 Controlled and Restricted Areas</td>
</tr>
<tr>
<td><strong>Design Basis Threat (DBT) for Terrorism (i.e. External/Internal Blast, External/ Internal CBRN Release, External/Internal Armed Attack and Physical Attack or Tampering of IT Systems)</strong></td>
<td>1.1 Top Management Commitment, 1.2 Policy, 2.1 Risk Assessment</td>
</tr>
<tr>
<td><strong>Business Impact Assessment</strong></td>
<td>2.1 Risk Assessment, 2.3 Incident Preparedness, 2.5 Continuity of Operations, 7.2 Evaluation</td>
</tr>
</tbody>
</table>

**TABLE 1: DOCUMENTATION REVIEW LIST**

### 5.1.2. Document Rating Scale

In the assessment report, rate the documents that provide or do not provide evidence of a best practice and comment on items missing or incomplete. A simple scale used in the BPATS Assessment Tool is listed here:

- **AA**  Available, meets needs and attached
- **AR**  Available, meets needs but restricted and not attached
- **AI**  Available but Incomplete
- **NP**  Not Present

Assessors should rely on their training and experience to make this Rating determination. When numerous records are available, assessors should review a sample of those records. For example, if...
security officers are required to fill out a checklist for inspections, assessors should review a reasonable number of the checklists.

As part of this documentation review, you should determine if the evidence contained in the documentation comes from appropriate sources. That is, are there signed and dated internal records related to the security system and after-action reports from third-party organizations?

5.2. Site Visit

The second step in the assessment process is a site visit. The purpose of the site visit is to record how well the Building Security Program (within the limits of the scope of the assessment) compares to each of the 411 Common Security Practices and the 24 BPATS or other applicable security practices. You can determine this by observing the site layout and design, interviewing the facility staff and/or contractors, witnessing operations, and reviewing additional documentation found during the tour.

One underlying question is: “Do the plans and procedures match the current operations?” Pay close attention to issues or areas of uncertainty discovered during the documentation review.

5.2.1. Site Visit Plan

Before the site visit, the you should develop a site visit plan. The site visit plan serves as the road map for the visit and sets expectations for both parties. The OSAI recommends including the Site Visit Plan in facility assessment reports as evidence of an organized assessment.

At a minimum, the Site Visit Plan should include the following:

- Tour all aspects of the facility and its security systems;
- Interview facility staff and/or contractors;
- Compare policy to current operations; and
- Identify facility assets, threats, and vulnerabilities.

The site visit plan serves as the road map for the site visit and sets expectations for both parties.

A key step in this process is to coordinate with the facility before the visit. Pre-visit coordination (both by e-mail and teleconference) can be used to set objectives based on the facility’s characteristics, notify the site of the expected duration of the visit, and identify the resources needed to conduct the assessment. Thorough preparation will optimize time spent at the site.

5.2.2. Assets, Functions, Infrastructure

One way to gain different perspectives of the facility during the site visit is to look at the facility’s assets, functions, and infrastructure separately. This simplifies an understanding of how the facility may be affected by a terrorist act. The below table lists areas to consider in each category. (See TABLE 2: ASSETS, FUNCTIONS, INFRASTRUCTURE)
### Table 2: Assets, Functions, Infrastructure

<table>
<thead>
<tr>
<th>Assets</th>
<th>Functions</th>
<th>Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Occupants</td>
<td>• Building Management</td>
<td>• Site</td>
</tr>
<tr>
<td>• Materials</td>
<td>• Security Operations and Management</td>
<td>• Architecture</td>
</tr>
<tr>
<td>• Replacement Value</td>
<td>• Security Forces</td>
<td>• Building Envelope</td>
</tr>
<tr>
<td>• Local / Regional Impact</td>
<td>• Planning and Exercises</td>
<td>• Structural Components and Systems</td>
</tr>
<tr>
<td></td>
<td>• Engineering Operations and Maintenance</td>
<td>• Mechanical / Electrical / Utilities</td>
</tr>
<tr>
<td></td>
<td>• Business Continuity</td>
<td>• IT and Communication</td>
</tr>
<tr>
<td></td>
<td>• Vendors</td>
<td>• Fire Alarm Systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Security Systems</td>
</tr>
</tbody>
</table>

Assets include the occupants and materials. Consider the replacement value of those assets, and also consider the local/regional impact from the loss of those assets. You should consider not only the occupants during a normal day, but also at peak levels, when employees, visitors, and vendors are on site. This number should not include brief influxes in population as an occasional conference (or similar event), unless the facility is intended for use in such a manner (like a conference center) and the population is part of normal business. Remember to consider high value or bulk materials present and their replacement value.

Functions include Building Management, Security Operations and Management, Facility Engineering and others. Consider which functions have to operate 24/7 and which may be delayed following an event.

Finally, you need to look at the site’s infrastructure. This is a challenging task, since the infrastructure is a complex interrelated system. Look at each component separately, but also consider how each infrastructure component functions in related systems and in the larger system as a whole. For example, mechanical/electrical/utilities will be closely linked with everything from IT and Communication, to fire alarms, and security systems.

Get in the habit of looking at different systems multiple times from different perspectives as you conduct your visit.

#### 5.2.3. Tour Checklist

Before the site visit, your assessment team should develop a Tour Checklist. Establishing a checklist is a good method for ensuring you accomplish your site visit goals.

First, you need to ensure that the tour will meet the assessment objectives and scope, as well as the Best Practice requirements. For example, there are practices concerning parking. If the parking area is in the scope of the assessment, then it needs to be part of the tour. If the building uses a parking facility in a separate building across the street and it is not in the scope of the assessment, then the parking practices are non-applicable, and the parking facility does not need to be on the site tour checklist.
Second, you need to observe the building’s security program in action. Ways to do this are to watch security staff perform their duties, request to witness common security activities, such as visitor processing, and observe a normally scheduled test of security equipment, systems, or capability.

Third, you should confirm that documented plans, policies, and procedures reflect actual practice.

Finally, the tour checklist should include looking at adjacent facilities. These nearby facilities may increase target attractiveness, or you may be at risk from “collateral damage” from an attack on an adjacent site.

The following list is a starting point for planning your visit, and may be adapted as needed:

- Adjacent Facilities
- Air Intakes
- Building Perimeter
- Data / Telephone Systems: Centers, Demarcation Point, Distribution Systems and Closets
- Emergency Generator/ fuel
- Emergency Operations Center
- Engineering Control Center
- Exterior Entrances
- Fire Control Center
- Fuel Storage
- Lobbies
- Loading Dock
- Mailroom
- Major Mechanical, Electrical and Plumbing Systems
- Parking Areas
- Roof Access
- Security Control Center
- Warehouse
- Water Supply

### 5.2.4. Threats

Building security programs are affected by changing threats. The topic of “Threats” is addressed in eight of the Common Security Practices and an understanding of unique threats to the facility is an important part of an assessment. As part of the site visit, ask the building owner / representative to review their threat assessment. If they have a Threat Assessment, analyze it with them. If appropriate, include it in your assessment.

If the owner does not have a threat assessment, conduct an analysis with them and determine the threats you will consider in your assessment. A good tactic for doing this is to first list all possible threats and then tailor that list for the facility.

For example, first consider all possible threats to the facility, such as the below extract from: The Risk Management Process: An Interagency Security Committee Standard Appendix F: Forms & Templates,
5.2.5. Comparison analysis to Best Practices for Anti-Terrorism Security (BPATS)

During the site visit, conduct a comparison analysis of the current security practices to the BPATS and their related Common Security Practices. See BEST PRACTICES FOR ANTI-TERRORISM SECURITY (BPATS) LIST FOR COMMERCIAL OFFICE BUILDINGS, DHS Office of SAFETY Act Implementation, for the complete BPATS listing. For conducting the comparison, it is recommended to use the automated BPATS.
worksheets in the online tool: *BPATS Assessment Tool for Commercial Facilities*. The tool may be found at: [https://bpatsassessmenttool.nibs.org](https://bpatsassessmenttool.nibs.org)

To organize the comparison, the following taxonomy has been established (See Diagram 1: BPATS TAXONOMY):

- At the highest level there are 7 Practice Categories used to organize the 24 Best Practices for Anti-Terrorism Security or BPATS. Each Practice Category contains two to five related BPATS, for a total of 24 BPATS.
- Under each individual BPATS, there are three to 60 associated Common Security Practices for a total of 411 Common Security Practices.

Each BPATS includes: A Scope Statement; a Best Practice Statement, which identifies the outcome specified by the best practice (in other words, the requirements); and a list of Common Security Practices. (See Diagram 2, Extract of BPATS 1.1 Top Management Commitment)
The Common Security Practices are suggested anti-terrorism actions, procedures, methods, or systems used to execute the outcome specified by the best practice. BPATS are not compliance items, but goal-oriented statements of anti-terrorism security objectives. Conducting a comparison is a way to collect information, and this requires that you ask more than just “Yes” or “No” questions. Analyzing how the buildings security program compares with a Best Practice should result in specific and detailed findings.

As such, this comparison process requires an experienced assessor with prior knowledge of security engineering principles. Assessor’s need to have an understanding of concepts, such as “progressive collapse”, “blast effects”, and “biological and chemical properties” to be effective.

Other concepts include, “layered defense” and “detect, assess, delay, and respond”. You will need to use this knowledge as a lens for viewing the security practices discussed in the BPATS.

The BPATS list is not finite: i.e. it does not cover local building code, life safety, or HAZMAT requirements. However, any open violations of these requirements should be considered. Assessors may also consider security practices not listed.

5.2.6. Best Practices for Anti-Terrorism Security (BPATS) Ratings

During and/or following the site visit, complete an assessment worksheet for each of the BPATS and their related Common Security Practices. The assessment worksheet has a place to record a rating for each BPATS and Common Security Practice and also your rationale for the rating. There is no set number of Common Security Practices necessary to achieve a “Satisfactory” BPATS rating. You will need to rely on your expertise and experience to rate the comparison of the practice.

The recommended rating scale is: Satisfactory, Partial, Unsatisfactory and Uncertain. In your assessment report, any Partial or Unsatisfactory ratings should have comments to explain your finding and a recommended mitigation.

The criteria for each rating is listed in the following table. (See TABLE 3: BPATS RATING SYSTEM). An Uncertain rating will be further explained below.

<table>
<thead>
<tr>
<th>Satisfactory</th>
<th>Partial</th>
<th>Unsatisfactory</th>
<th>Uncertain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence indicates security system has satisfied the BPATS</td>
<td>Evidence indicates most security systems have satisfied the BPATS</td>
<td>Evidence clearly indicates security system has not satisfied the BPATS, or</td>
<td>Unknown</td>
</tr>
<tr>
<td>Evidence is credible, coherent and fully understood</td>
<td>Some evidence is credible, coherent and fully understood</td>
<td>Evidence is not credible or not coherent, or</td>
<td>Unknown</td>
</tr>
<tr>
<td>Evidence does not have obvious internal inconsistencies or inconsistencies with other evidence</td>
<td>Some evidence does not have obvious internal inconsistencies or inconsistencies with other evidence</td>
<td>There is significant inconsistency in the evidence</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

TABLE 3: BPATS RATING SYSTEM
An “uncertain” rating applies when the assessor cannot determine from the documentation review or the site visit if the facility security system is comparable to the BPATS under review. This rating is appropriate when more or better information is needed to rate the system “satisfactory”, “partial” or “unsatisfactory.” For each uncertain rating, the assessor should:

- Identify the degree to which it affects the system’s anti-terrorism capability;
- Identify a way to resolve the issue (if possible);
- Assess the impact on the evaluation if the issue is not resolved;
- Document the missing information in the report.

Assessors will rely on their expertise and experience to rate the capability and effectiveness of the facility security program. Remember the ratings justification must be evidence based. This may be accomplished by any of the following methods:

- Support the rating by referencing documentation, records, observations made during the site visit or by other forms of evidence.
- Reference any common security practices implemented. Be detailed in your explanation.
- List assumptions, if any, made while rating a best practice. Describe any inherent risks associated with those assumptions.
- For “Uncertain” or “Unsatisfactory” ratings, list what other information, if any, is needed to change the rating.

5.3. Report Development

Following the documentation review and site visit, the next step is to complete an assessment report. The purpose of the assessment report is to provide a record of the evaluation of the full scope of the assessment, not generalities. The report should contain the information listed below.

- Executive Summary
- Facility Overview
  - Threat Synopsis
    - General Threats
    - Unique Threats to the Facility
  - Site Details
  - Ownership, Management and Subagents
  - Key Assessment Participants
- Assessment Approach
  - Assessment Date
  - Assessment Scope
  - Assessment Team
Field Guide: Conducting BPATS Based Assessments of Commercial Facilities

- Assessment Findings
  - Document Review
  - Prioritized Consolidated Concerns
  - Consolidated List of Innovative Practices
  - Parts of the Anti-Terrorism Security System Not Assessed
  - Difficulties of Obstacles Encountered
- Confidentiality Agreement
- Signature
- Appendix A: Pictures / Diagrams
- Appendix B: Comprehensive Building Assessment Best Practices for Anti-Terrorism Security (BPATS)

Four areas to highlight with additional guidance are the Assessment Team entry, the Executive Summary, the Assessment Worksheets, and Lessons Learned.

### 5.3.1. Assessment Team
Assessments carried out by an independent, experienced and knowledgeable assessor(s) may enhance the significance given to an assessment. Assessors are encouraged to include a copy of their resume in the report.

Evidence of an experienced and knowledgeable assessor may include four years of progressive experience in the physical security field and a bachelor’s degree or higher from an accredited institution of higher education or completion of a building security professional certification program such as those offered by ASIS International, the Building Owners and Managers Institute International, or other professional societies. (i.e. Physical Security Professional (PSP), or Certified Protection Professional (CPP). Assessors should also have experience / training relevant to the seven knowledge domains of the Best Practices for Anti-Terrorism Security (BPATS).

For assessments using the online BPATS Based Assessment Tool, it has a place to include the assessor’s qualifications. The tool includes the Professional Summary, Education, Training, & Certifications, and Completion Date of BPATS Based Assessment Tool training.

### 5.3.2. Executive Summary
The purpose of the Executive Summary is to provide the reader with a brief but comprehensive overview of the report’s key findings on the facility security program’s anti-terrorism capability. It should include the overall ratings and findings of the 24 BPATS as well as observations and comments of those ratings. The Executive Summary should include notable strengths or positive aspects of the facility’s security. Finally, the Executive Summary should include any major difficulties or obstacles that were encountered during either the document review or the site visit.

### 5.3.3. Assessment Worksheets
In the recommended report outline, worksheets covering the 24 BPATS and the 411 Common Security Practices are included as an appendix. Each Worksheet includes an overall BPATS rating (Satisfactory, Partial, Unsatisfactory, Uncertain), summary comments on documentation, Common Security Practices, and observations of the BPATS, comments on assumptions, and comments on "Uncertain" or "Unsatisfactory" BPATS ratings. The worksheets also include an Observation and Recommendation for each Common Security Practice not rated “Satisfactory”.

Prepared by National Institute of Building Sciences
These sheets make up the main bulk of the assessment report.

5.3.4. Lessons Learned

The following Lessons Learned were developed through discussions with the OSAI concerning assessment reports.

- One of the first things to remember is that you shouldn’t try to protect the facility with a perfect report. This type of report lacks credibility, since it is likely that most facilities will have some areas that can be improved upon. Findings may be corrected in the next step, when the Owner/Operator develops and executes a mitigation plan.
- All assessments need to be based on solid, credible evidence that stems from the documentation review and site visit. Be specific, not general.
- Also remember that the assessment ratings are not “all or nothing” for the entire site. There may be parts of the facility that are better protected than others. For example, a facility’s main tower may have significantly more layers of security than a commercial plaza.
- When it comes to writing the report, stick to just the facts; don’t include any marketing information or content not directly relevant to the assessment.
- Finally, highlight Assessor Credentials in the report.

5.3.5. Routing of Reports

If there is a terrorist incident, injured parties may request access to assessment reports to see if terrorists exploited a weakness that had been previously identified. Written records of a security assessment can be viewed as a double-edged sword. No records or poor records may make it difficult for a facility to credibly assert that it regularly assessed its security program and mitigated findings. However, an assessment program coupled with a mitigation strategy may show a stronger due diligence by the Owner.

You should also recognize that not all information is treated the same. There may be confidential business information or privileged information and Personally Identifiable Information (PII) that may require special steps to protect. For building owners/operators that submit SAFETY Act applications to OSAI, documents provided in support of those applications will be treated as SAFETY Act Confidential Information (SACI). Those protections do not apply to the assessment copy sent to and held by the Building Owner / Operator.

As part of the Report Phase, coordinate with the owner/operator to identify their information protection policies and routing instructions for the assessment documents. For example, they may have you pass information to their General Counsel.

Note: The Assessment report is just one part of a SAFETY Act application. The use of the BPATS tool and assessment results help building owners take the first steps in preparing an application for SAFETY Act protections, should the building owner wish to apply.
6. Owner/Operator Actions

Owner/Operator actions include establishing an assessment scope statement, selecting an assessment team, supporting the assessment and post assessment analysis / mitigation / documentation.

The following diagram depicts the process (See Diagram 3: ASSESSMENT PROCESS):

![Diagram 3: Assessment Process](image)

6.1. Post Assessment Actions: Mitigation, Deferred Mitigation, Acceptance of Risk

After the assessment is completed and submitted to the Owner, the next step is analysis and mitigation decision-making: Mitigation, Deferred Mitigation, Acceptance of Risk.¹

In the assessment report, the owner is provided assessment findings including:

- Document Review
- Prioritized Consolidated Concerns
- Consolidated List of Innovative Practices
- Parts of the Anti-Terrorism Security System Not Assessed
- Difficulties of Obstacles Encountered

Each of these findings should be addressed in a post assessment mitigation / risk acceptance summary. This records the owners post assessment actions:

- Analysis and evaluation of the risk associated with each finding

¹For a detailed discussion on incremental protection for existing commercial buildings see FEMA publication “Risk Management Series, Incremental Protection for Existing Commercial Buildings from Terrorist Attack. Providing Protection to People and Buildings”. FEMA 459 / April 2008
• Determination of appropriate ways to eliminate the hazard, or control risk if the hazard cannot be eliminated
• Completion of mitigation actions
• Deferred mitigation
• Re-evaluation of each finding after mitigation based on compliance with mitigation decisions

Where owners decide to defer mitigation, or take no action following appropriate risk analysis or for other reasons, it is recommended that those decisions are reviewed by the senior management body of the organization and a formal minute is recorded of both the decision reached and the reasons for reaching it.

Note: The BPATS and CSP lists are not intended to be used as rigid decision-making criteria to declare a facility ‘safe’ or ‘not safe’ from terrorism solely based on a single finding. The use of the BPATS tool and assessment results help building owners take the first steps in preparing an application for SAFETY Act protections, should the building owner wish to apply.

6.2. Recording Post Assessment Actions in the BPATS Tool

An Owner level user account in the BPATS assessment tool allows the owner to import the encrypted assessment file, view the assessment section by section as well as in five report formats, enter comments on each finding in the document review section and the BPATS section and make general comments on other aspects of the assessment. The Owner can then produce a report summarizing the owner’s actions and the resulting improvement to the status of the facility. This is called the “Consolidated List of Owner/Representative Comments” report.

Steps to use the BPATS Tool to record Owner actions:

1. The Owner establishes an Owner level user account and gives the assessor their account code.
2. The Assessor grants access to the assessment to the Owner in the system.
3. Owner receives the encrypted assessment file form the assessor.
4. The Owner logs in to the BPATS Tool and imports the encrypted assessment file.
5. The Owner views the assessment section by section or prints out the findings and uses the list to facilitate planning for Mitigation or Deferred Mitigation / Acceptance of Risk. The owner may also enter a “Disputed” rating and provide comments on uncertainties or missing information that would contradict an assessor’s finding.
6. The Owner conducts mitigation.
7. The Owner records Mitigation, Deferred Mitigation / Acceptance of Risk or disputed rating comments on each finding in the document review section, the BPATS section and the Summary section of the assessment in the report titled: Consolidated List of Owner/Representative Comments.
6.3. Samples of Owner Comments to include operational procedures and technology

Owner comments should reference the BPATS finding, be evidence based and supported by documentation, records and observations made after mitigation. The following are samples of mitigation strategies and Owner comments, to include operational procedures and technology.

- Project how recommended actions improve the situation. For example:

  Access control to telecommunication room doors was identified in finding 3.2.05 as a weakness. In January XXXX a new XXX brand access control system was established on all telecommunication room doors. A person breaking into a room will now be detected and assessed by the security force. Response procedures have been prepared and coordinate with tenants.

- Identify the key elements for believing there is or is not justification to take action. For example:

  Finding 6.1.02 stated that glass should be selected and designed to meet the security requirements of the threat(s), threat locations and vulnerabilities identified in the site risk assessment. Based on this finding, a risk assessment, was conducted by XXX on XX/XX/XXXX. The assessment determined the highest risk was to the conference room windows facing XXX street due to their proximity to the street and that they overlook a mass gathering area. (See attached Risk Assessment XXXX). These windows were fitted with fragment retention films on XX/XX/XXXX to mitigate the greatest risk. (See project description in attachment XXX.)

- Identify key uncertainties and what additional information could reduce the uncertainties. For example:

  Information on the training status of the security force was not available to the assessor during the assessment period. On XX/XX/XXXX the Security Force contractor supplied a training report for the status of the Security force. All personnel were found in compliance.

- Identify newly implemented security technologies. For example:

  The control of master keys to the utility rooms and perimeter doors was a weakness in the assessment report, BPATS 2.3.20. An electronic key box system has been established for the cleaning crew and all utility and perimeter door locks have been reconfigured with a smart key system.
This section of the FEDERAL REGISTER contains regulatory documents having general applicability and legal effect, most of which are keyed to and codified in the Code of Federal Regulations, which is published under 50 titles pursuant to 44 U.S.C. 1510.

The Code of Federal Regulations is sold by the Superintendent of Documents. Prices of new books are listed in the first FEDERAL REGISTER issue of each week.

DEPARTMENT OF HOMELAND SECURITY
Office of the Secretary
6 CFR Part 25
[USCG–2003–15425]
RIN 1601–AA15

Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act)

AGENCY: Office of the Secretary, Department of Homeland Security.

ACTION: Final rule.

SUMMARY: This final rule implements Subtitle G of Title VIII of the Homeland Security Act of 2002—the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (“the SAFETY Act” or “the Act”), which provides critical incentives for the development and deployment of anti-terrorism technologies by providing liability protections for providers of “qualified anti-terrorism technologies.” The purpose of this rule is to facilitate and promote the development and deployment of anti-terrorism technologies that will save lives. The final rule amends the interim rule to incorporate changes resulting from the comments.

DATES: This final rule is effective July 10, 2006.

ADDRESSES: You may submit comments identified by Coast Guard docket number USCG–2003–15425 or RIN 1601–AA15, to the Docket Management Facility at the Department of Transportation, by one of the following methods:

(2) Mail: Docket Management Facility, U.S. Department of Transportation, 400 Seventh Street, SW., Washington, DC 20590–0001.
(3) Fax: 202–493–2251.
(4) Delivery: Room PL–401 on the Plaza level of the Nassif Building, 400 Seventh Street, SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202–366–9329.

Instructions: Comments and materials received from the public, as well as documents mentioned in this preamble as being available in the docket, are part of docket USCG–2003–15425 and are available for inspection or copying from the Docket Management Facility, U.S. Department of Transportation, room PL–401, 400 Seventh Street, SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday except Federal holidays. You may also find this docket on the Internet at http://dms.dot.gov. You may also access the Federal eRulemaking Portal at http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: If you have questions on this final rule, contact the Director of the Office of SAFETY Act Implementation, Science and Technology, Department of Homeland Security, telephone 703–575–4511. If you have questions on viewing or submitting material to the docket, call Dorothy Beard, Chief, Dockets, Department of Transportation, telephone 202–366–5149.

SUPPLEMENTARY INFORMATION:

Capitalized terms appearing in this preamble shall have the meanings ascribed to such terms in §25.2 of this final rule. This section is organized as follows:

Table of Contents

I. Analysis of the SAFETY Act
   A. Background
   B. Statutory and Regulatory History and Analysis
   C. Government Contractor Defense
   D. Exclusive Federal Jurisdiction and Scope of Insurance Coverage
   E. Relationship of the SAFETY Act to Indemnification Under Public Law 85–804

II. Discussion of Changes and Comments
   A. Confidentiality of Information
   B. Application Preparation Burden
   C. Certifying “accuracy and completeness”
   D. Conditions on Designations
   E. Significant Modification to a Qualified Anti-Terrorism Technology

F. Exclusive Responsibility for Government Contractor Defense, Definitions of Fraud and Willful Misconduct
G. Definition of an “Act of Terrorism”
H. Retroactive Designation
I. Bias Toward Product-Based Anti-Terrorism Technologies
J. Scope of Insurance Coverage
K. Interactions With Public Law 85–804
L. Prioritization of Evaluations
M. Standards
N. Expiration of Designations
O. Appeal/Review of Decisions Regarding SAFETY Act Applications
P. Coordination With Government Procurements
Q. Pre-Application Consultations
R. Developmental Test & Evaluation Designations
S. Seller’s Continuing Obligations With Respect to Maintaining Insurance
T. Block Designations and Block Certifications
U. Reciprocal Waivers
V. Defereence Due to Other Federal or State Regulatory or Procurement Officials

III. Regulatory Requirements

A. Executive Order 12866
B. Regulatory Flexibility Act
C. Unfunded Mandates Reform Act of 1995
D. Executive Order 13132—Federalism
E. Paperwork Reduction Act

I. Analysis of the SAFETY Act

A. Background

Congress was clear, both in the text of the SAFETY Act and in the Act’s legislative history, that the SAFETY Act can and should be a critical tool in expanding the creation, proliferation and use of anti-terrorism technologies.

On July 11, 2003, the Department of Homeland Security (“DHS”) published its first proposed rules for implementation of the SAFETY Act (Notice of Proposed Rulemaking entitled “Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act)” (68 FR 41420), laying out its fundamental interpretive approach to the Act and requesting comment. On October 16, 2003, an interim rule governing implementation of the SAFETY Act was promulgated making certain changes to the proposed rules but again embracing many of the fundamental interpretive approaches proposed several months earlier (68 FR 59684). Subsequently, the Department published detailed procedural mechanisms for implementation of the Act and announced additional details relating to the process for filing and adjudicating applications.
The SAFETY Act program is now in its third year, and the Department has a substantial record of program performance to evaluate. While the Department concludes that the Department’s core legal interpretations of the Act’s provisions are fundamentally sound, experience in administering the program has demonstrated that certain of the procedural processes built to administer the Act can be improved. Shortly after being sworn in, Secretary of Homeland Security Michael Chertoff stated: “There is more opportunity, much more opportunity, to take advantage of this important law, and we are going to do that.” In the past year, the Department has instituted process improvements which have yielded positive initial results. In the first sixteen months of the SAFETY Act program, from October 2003 to February 2005, six technologies were designated Qualified Anti-Terrorism Technologies under the SAFETY Act. By contrast, since March 2005, 68 additional technologies have received SAFETY Act protections. This is a greater than ten-fold increase in SAFETY Act approvals in the past 14 months. In addition, the Department has instituted a program to run SAFETY Act reviews in parallel with key anti-terrorism procurement processes. 

Despite these recent improvements, further changes to Department rules and processes are necessary to ensure that the program achieves the results that Congress intended. With this final rule, the Department:

1. Further clarifies the liability protections available under the SAFETY Act;

2. States with greater specificity those products and services that are eligible for Designation as a Qualified Anti-Terrorism Technology;

3. Clarifies the Department’s efforts to protect the confidential information, intellectual property, and trade secrets of SAFETY Act applicants;

4. Articulates the Department’s intention to extend SAFETY Act liability protections to well-defined categories of anti-terrorism technologies by issuing “Block Designations” and “Block Certifications”;

5. Discusses appropriate coordination of SAFETY Act consideration of anti-terrorism technologies with government procurement processes; and

6. Takes other actions necessary to streamline processes, add flexibility for applicants, and clarify protections afforded by the SAFETY Act.

While this rule is indeed final, the Department remains committed to making future changes to the implementing regulation or to any element of the program that interferes with the purposes of the SAFETY Act. To that end, the Department seeks further comment on the specific issues identified herein.

Section I of this preamble reviews the Department’s longstanding legal interpretation of the SAFETY Act’s provisions and reviews the Act’s statutory and regulatory history. Section II addresses regulatory changes and outlines additional improvements in SAFETY Act processes and procedures that the Department will implement in the coming months that will improve administration of the Act. Section III addresses this rule’s compliance with other regulatory requirements.

B. Statutory and Regulatory History and Analysis

As part of the Homeland Security Act of 2002, Public Law 107–296, Congress enacted liability protections for providers of certain anti-terrorism technologies. The SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by creating a system of “risk management” and a system of “litigation management.” The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or sellers of anti-terrorism technologies from developing, deploying, and commercializing technologies that could save lives. The Act thus creates certain liability limitations for “claims arising out of relating to, or resulting from an act of terrorism” where Qualified Anti-Terrorism Technologies (as such term is defined in 6 CFR 25.2) have been deployed.

Together, the risk and litigation management provisions provide the following protections:

- Exclusive jurisdiction in Federal court for suits against the sellers of “Qualified Anti-Terrorism Technologies” (§ 863(a)(2));
- A limitation on the liability of sellers of Qualified Anti-Terrorism Technologies to an amount of liability insurance coverage specified for each Qualified Anti-Terrorism Technology, provided that sellers cannot be required to obtain any more liability insurance coverage than is reasonably available “at prices and terms that will not unreasonably distort the sales price” of the technology (§ 864(a)(2));
- A prohibition on joint and several liability such that sellers can only be liable for the percentage of non-economic damages that is proportionate to their responsibility (§ 863(b)(2));
- A complete bar on punitive damages and prejudgment interest (§ 863(b)(1));
- The reduction of a plaintiff’s recovery by the amount of collateral source compensation, such as insurance benefits or government benefits, such plaintiff receives or is eligible to receive (§ 863(c)); and
- A rebuttable presumption that sellers are entitled to the “government contractor defense” (§ 863(d)).

The Secretary’s designation of a technology as a Qualified Anti-Terrorism Technology (QATT) confers each of the liability protections identified above except the rebuttable presumption in favor of the government contractor defense. The presumption in favor of the government contractor defense requires an additional “Certification” by the Secretary under section 863(d) of the Act. In many cases, however, SAFETY Act Designation and Certification are conferred contemporaneously.

As noted above, the Designation of a technology as a Qualified Anti-Terrorism Technology confers all of the liability protections provided in the SAFETY Act, except for the presumption in favor of the government contractor defense. The Act gives the Secretary broad discretion in determining whether to designate a particular technology as a Qualified Anti-Terrorism Technology, although the Act sets forth the following criteria for consideration of a particular technology:

1. Prior United States Government use or demonstrated substantial utility and effectiveness;
2. Availability of the technology for immediate deployment;
3. The potential liability of the Seller;
4. The likelihood that the technology will not be deployed unless the SAFETY Act protections are conferred;
5. The risk to the public if the technology is not deployed;
6. Evaluation of scientific studies; and
7. The effectiveness of the technology in defending against acts of terrorism. It is not required that applicants satisfy all of the preceding criteria to receive SAFETY Act protections. Moreover, these criteria are not exclusive—the Secretary may consider other factors that he deems appropriate. The Secretary has discretion to give greater weight to some factors over others, and the relative weighting of the various criteria may vary depending upon the particular technology at issue and the threats that the particular technology is designed to address. The Secretary may, in his discretion, determine that failure to meet a particular criterion justifies denial of an application under the SAFETY Act. However, the Secretary is
not required to reject an application that fails to meet one or more of the criteria. Rather, the Secretary may conclude, after considering all of the relevant criteria and any other relevant factors, that a particular technology merits Designation as a Qualified Anti-Terrorism Technology even if one or more particular criteria are not satisfied. The Secretary’s considerations will also vary with the constantly evolving threats and conditions that give rise to the need for the technologies.

The SAFETY Act applies to a broad range of technologies, including products, services, and software, or combinations thereof, as long as the Secretary, as an exercise of discretion and judgment, determines that a technology merits Designation. The Secretary may designate a system containing many component technologies (including products and services) or may designate specific component technologies individually. Further, as the statutory criteria suggest, a Qualified Anti-Terrorism Technology need not be newly developed—it may have already been employed (e.g., “prior United States government use”) or may be a new application of an existing technology.

The SAFETY Act provides that, before designating a Qualified Anti-Terrorism Technology, the Secretary will examine the amount of liability insurance the Seller of the technology proposes to maintain for coverage of the anti-terrorism technology at issue. Under section 864(a), the Secretary must certify that the coverage level is appropriate “to satisfy otherwise compensable third-party claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed.” § 864(a)(1). While the Act provides the Secretary with significant discretion in this regard, the Secretary may not require the Seller to obtain liability insurance of more than the maximum amount of liability insurance reasonably available from private sources on the world market. Likewise, the Secretary may not require a Seller to maintain the cost of which would unreasonably distort the sales price of Seller’s anti-terrorism technologies. § 864(a)(2). Although the Secretary may permit the Seller to self-insure, he may not require the Seller to self-insure if appropriate insurance is unavailable. § 864(a)(2).

The Secretary does not intend to set a “one-size-fits-all” numerical requirement regarding required insurance coverage for all technologies that have been designated as QATTs. Instead, as the Act suggests, the inquiry will be specific to each application and may involve an examination of several factors, including without limitation the following: (i) The amount of insurance the Seller has previously maintained; (ii) the amount of insurance maintained by the Seller for other related technologies or for the Seller’s business as a whole; (iii) the amount of insurance typically maintained by Sellers of comparable technologies; (iv) data and history regarding mass casualty losses; and (v) the particular technology at issue. Once the Secretary concludes the analysis regarding the appropriate level of insurance coverage (which typically will include discussions with the Seller), the Secretary will provide a description of the coverage appropriate for the particular Seller of a Qualified Anti-Terrorism Technology to maintain. The Seller’s insurance certification may identify an appropriate amount of insurance coverage available under a comprehensive general liability policy or other liability insurance program. The insurance certification also may specify that the amount of insurance required to be maintained will be the amount of coverage available under the terms of the specific policy at issue. If, during the term of the Designation, the Seller desires to request reconsideration of that insurance certification due to changed circumstances or for other reasons, the Seller may do so and the Secretary is authorized to use the discretion described above to adjust insurance requirements appropriately. If the Seller fails to maintain coverage at the certified level, the liability protections of Act will continue to apply, but the Seller’s liability limit will remain at the certified insurance level. The Department recognizes that the market for insurance might change over time and seeks further comment on how the Department can and should address changes in insurance availability.

C. Government Contractor Defense

The SAFETY Act creates a rebuttable presumption that the government contractor defense applies to those Qualified Anti-Terrorism Technologies “approved by the Secretary” in accordance with certain criteria specified in § 863(d)(2). The government contractor defense is an affirmative defense that immunizes Sellers from liability for certain claims brought under § 863(a) of the Act. See § 863(d)(1). The presumption of this defense applies to all “approved” Qualified Anti-Terrorism Technologies for claims brought in a “product liability or other lawsuit” and “arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies * * * have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller.” Id. While the government contractor defense is a judicially-created doctrine, section 863’s express terms supplant the requirements in the case law for the application of the defense. First, and most obviously, the Act expressly provides that the government contractor defense is available not only to government contractors, but also to those who sell to State and local governments or the private sector. See § 863(d)(1) (“This presumption of the government contractor defense shall apply regardless of whether the claim against the Seller arises from a sale of the product to Federal Government or non-Federal Government customers.”) Second, Sellers of Qualified Anti-Terrorism Technologies need not design their technologies to federal government specifications in order to obtain the government contractor defense under the SAFETY Act. Instead, the Act sets forth criteria for the Department’s Certification of technologies. Specifically, the Act provides that before issuing a Certification for a technology, the Secretary will conduct a “comprehensive review of the design of such technology and determine whether it will perform as intended, conforms to the Seller’s specifications, and is safe for use as intended.” § 863(d)(2). The Act also provides that the Seller will “conduct safety and hazard analyses” and supply such information to the Secretary. Id. This express statutory framework thus governs in lieu of the requirements developed in case law for the application of the government contractor defense. Third, the Act expressly states the limited circumstances in which the applicability of the defense can be rebutted. The Act provides expressly that the presumption can be overcome only by evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the course of the Secretary’s consideration of such technology. See § 863(d)(1) (“This presumption shall only be overcome by evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the course of the Secretary’s consideration of such technology under this subsection.”)

The applicability of the government contractor defense to particular technologies is thus governed by these express provisions of the Act, rather than by the judicially-developed criteria
for applicability of the government contractor defense outside the context of the SAFETY Act. While the Act does not expressly delineate the scope of the defense (i.e., the types of claims that the defense bars), the Act and the legislative history make clear that the scope is broad. For example, it is clear that any Seller of an “approved” technology cannot be held liable under the Act for design defects or failure to warn claims, unless the presumption of the defense is rebutted by evidence that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the course of the Secretary’s consideration of such technology. In Boyle v. United Technologies Corp., and its progeny, the Supreme Court has ruled that the government contractor defense bars a broad range of claims. For example, the Supreme Court in Boyle concluded that “state law which holds Government contractors liable for design defects” can present a significant conflict with Federal policy (including the discretionary function exception to the Federal Tort Claims Act) and therefore “must be displaced.” Boyle v. United Technologies Corp., 487 U.S. 500, 512 (1988). The Department believes with the SAFETY Act that Congress incorporated government contractor defense protections outlined in the Supreme Court’s Boyle line of cases as it existed on the date of enactment of the SAFETY Act, rather than incorporating future developments of the government contractor defense in the courts. Indeed, it is difficult to imagine that Congress would have intended a statute designed to provide certainty and protection to Sellers of anti-terrorism technologies to be subject to future developments of a judicially-created doctrine. In fact, there is evidence that Congress rejected such a construction. See, e.g., 148 Cong. Rec. E2080 (November 13, 2001) (statement of Rep. Army) (“[Companies] will have a government contractor defense as is commonplace in existing law.”) (emphasis added).

Procedurally, the presumption of applicability of the government contractor defense is conferred by the Secretary’s Certification of a Qualified Anti-Terrorism Technology specifically for the purposes of the government contractor defense. This Certification is an act separate from the Secretary’s issuance of a Designation for a Qualified Anti-Terrorism Technology and confers additional benefits to Sellers. Importantly, Sellers may submit applications for both Designation as a Qualified Anti-Terrorism Technology and Certification for purposes of the government contractor defense at the same time, and the Secretary may review and act upon both applications contemporaneously. The distinction between the Secretary’s two actions is important, however, because the approval process for the government contractor defense includes a level of review that is not required for the Designation as a Qualified Anti-Terrorism Technology. In appropriate cases, Sellers may obtain the protections that come with Designation as a Qualified Anti-Terrorism Technology even if they have not satisfied the additional requirements for the government contractor defense.

In an effort to provide greater clarity, the Department intends to publish guidance regarding its interpretation of the government contractor defense and the Supreme Court’s Boyle line of cases as it existed on the date of enactment of the SAFETY Act.

D. Exclusive Federal Jurisdiction and Scope of Insurance Coverage

The Act creates an exclusive Federal cause of action “for any claim for loss of property, personal injury, or death arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller.” § 863(a)(1). The best reading of § 863(a), and the reading the Department has adopted, is that

(1) Only one cause of action exists for loss of property, personal injury, or death for performance or non-performance of the Seller’s Qualified Anti-Terrorism Technology in relation to an Act of Terrorism,

(2) Such cause of action may be brought only against the Seller of the Qualified Anti-Terrorism Technology and may not be brought against the buyers, the buyers’ contractors, downstream users of the Qualified Anti-Terrorism Technology, the Seller’s suppliers or contractors, or any other person or entity, and

(3) Such cause of action must be brought in Federal court. The exclusive Federal nature of this cause of action is evidenced in large part by the exclusive jurisdiction provision in § 863(a)(2).

The Department believes Congress did not intend through the Act to increase rather than decrease the amount of litigation arising out of or related to the deployment of Qualified Anti-Terrorism Technology. Rather, Congress balanced the need to provide recovery to plaintiffs against the need to
ensure adequate deployment of anti-terrorism technologies by creating a cause of action that provides a certain level of recovery against Sellers, while at the same time protecting others in the supply chain.

E. Relationship of the SAFETY Act to Indemnification Under Public Law 85–804

The Department recognizes that Congress intended that the SAFETY Act’s liability protections would substantially reduce the need for the United States to provide indemnification under Public Law 85–804 to Sellers of anti-terrorism technologies. The liability protections of the SAFETY Act should, in many circumstances, make it unnecessary to provide indemnification to Sellers. The Department recognizes, however, that there are circumstances in which both SAFETY Act coverage and indemnification are warranted. See 148 Cong. Rec. E2080 (statement by Rep. Armey) (November 13, 2002) (stating that in some situations the SAFETY Act provides protections “to complement other government risk-sharing measures that some contractors can use such as Pub. L. 85–804”). In recognition of this close relationship between the SAFETY Act and indemnification authority, in section 73 of Executive Order 13286 of February 28, 2003, the President amended the existing Executive Order on indemnification—Executive Order 10789 of November 14, 1958, as amended. The amendment granted the Department of Homeland Security authority to indemnify under Public Law 85–804. At the same time, it requires that all agencies—not just the Department of Homeland Security—follow certain procedures to ensure that the potential applicability of the SAFETY Act is considered before any indemnification is granted for an anti-terrorism technology. Specifically, the amendment provides that Federal agencies cannot provide indemnification “with respect to any matter that has been, or could be, designated by the Secretary of Homeland Security as a qualified anti-terrorism technology” unless the Secretary of Homeland Security has advised whether SAFETY Act coverage would be appropriate and the Director of the Office of Management and Budget has approved the exercise of indemnification authority. The amendment includes an exception for the Department of Defense where the Secretary of Defense has determined that indemnification is “necessary for the timely and effective conduct of United States military or intelligence activities.”

II. Discussion of Changes and Comments

The Department received 16 sets of comments to the interim rule during the comment period and has made substantive and stylistic changes in response to those comments. The Department considered all of the comments received and the Department’s responses follow.

A. Confidentiality of Information

Eight commenters expressed dissatisfaction with the Department’s stated policy with regard to safeguarding proprietary information (including business confidential information) submitted as part of a SAFETY Act application. Some commenters desired the Department to declare that SAFETY Act application contents are “voluntary submissions” for purposes of determining whether the Critical Infrastructure Information Act applies. Commenters also noted that Exemption 4 of FOIA protects “trade secrets or commercial or financial information from a person that is privileged or confidential.”

The Department remains committed to the vigorous protection of applicants’ submissions and confidential information. One applicant suggested that the Department “adopt a general presumption of confidential treatment of all SAFETY Act applications, evaluations and studies of such applications, underlying decisional documentation, and application rejection notices.” This has been the Department’s intention, policy, and practice from the outset. DHS is committed to taking all appropriate steps to protect the proprietary information of applicants consistent with applicable FOIA exemptions and the Trade Secrets Act (18 U.S.C. 1905). As an example of this commitment, those engaged in evaluating applications are required to enter into appropriate nondisclosure agreements. In addition, prior to being granted access to any proprietary information associated with an application or its evaluation, each potential evaluator is examined for potential conflicts of interest. Finally, the Department’s conflict of interest and confidentiality policies apply to everyone associated with SAFETY Act implementation.

Underlying this commitment to protect an applicant’s information are various Federal civil and criminal laws that apply to unauthorized disclosure of SAFETY Act confidential materials, including the Trade Secrets Act and 18 U.S.C. Chapter 90 (Protection of Trade Secrets, especially section 1831—Economic Espionage, and section 1832—Theft of Trade Secrets). These laws establish criminal penalties for disclosing proprietary data under various circumstances. There are also relevant state laws, including versions of the Uniform Trade Secrets Act adopted in the District of Columbia, the State of Maryland, the Commonwealth of Virginia, and 39 other states. In addition, sensitive homeland security information, including information regarding vulnerabilities of critical infrastructure can be entitled to certain statutory protections under sections 892(a)(1)(B), 892(b)(3), 892(f) of the Homeland Security Act of 2002, Sensitive Security Information under 49 U.S.C. 40119, 49 CFR part 1520 and FOIA Exemption 3 (among other FOIA exemptions).

The Department also believes that all information that is submitted as part of an application, including the fact that a particular entity has submitted an application, is confidential commercial information under the tests established in National Parks & Conservation Association v. Morton, 498 F.2d 765 (D.C. Cir. 1974), and its progeny. In particular, much or all of this information qualifies as confidential under both the “competitive harm” prong of the test, and the “third prong” of government interest and program effectiveness.

The Department will assert appropriate exemptions, including, as applicable, FOIA Exemptions 1 through 4 in declining to disclose under FOIA any information concerning the source of a SAFETY Act application or the contents of applications. This policy is now reflected in the rule at section 25.10 of this final rule. In addition, the Department will work with applicants to ensure that no proprietary information is published in connection with an announcement of a Block Designation (pursuant to §25.6(i) of this final rule), DHS’s publication of the Approved Product List for Homeland Security (pursuant to §25.8(k) of the final rule) or the voluntary publication by DHS of issued Designations. Moreover, the Government does not, at this time, intend to “portion mark” information contained in the application, or associated case file, to delineate between protected proprietary information (also referred to as “SAFETY Act Confidential Information”) and other less sensitive data in the application. Instead the entirety of the application will be treated as confidential under appropriate law. It is the Department’s
believe that requiring the reviewer to portion mark at the time of submission would greatly impact efficiency and applicants’ confidence in the integrity of protections for proprietary information, and that such a practice does not reflect the requirements of applicable confidentiality protections. The Department has established internal security procedures for handling technical, business, and insurance information that is submitted in connection with a SAFETY Act application. Certain of the measures the Department has instituted to safeguard proprietary information are reflected in 6 CFR 25.10. All applications, whether paper or electronic, will be subject to stringent safeguards. In obtaining the input of subject matter experts and evaluators that analyze SAFETY Act applications, the Department will only seek input from individual experts or evaluators and will not consult any committee in the process of reviewing SAFETY Act applications. Finally, the Department recognizes that information submitted to SAFETY Act applications may constitute Protected Critical Infrastructure Information pursuant to sections 211–215 of the Homeland Security Act of 2002. The Department is in the process of revising its Protected Critical Infrastructure Information regulations and anticipates providing further information on this subject in the near future.

B. Application Preparation Burden

Six commenters expressed concern that the amount and type of information required by the SAFETY Act Application Kit is extremely burdensome, if not prohibitively so, and that only large companies have the resources necessary to respond to each of the questions. Commenters also expressed the opinion that some of the information being requested—particularly financial information—is not relevant to the evaluation of applications against the criteria of the Act.

The Department recognizes that the SAFETY Act Application Kit utilized to date poses significant burdens for applicants. We are very sensitive to concerns about the application process and the difficulty of preparing and submitting a SAFETY Act application. The Department specifically solicited comments on the SAFETY Act Application Kit and application process set forth in the interim rule. In addition, the Department released for comment a revised SAFETY Act Application Kit in December 2004. Based on both the comments received concerning the SAFETY Act Application Kit as well as the experience of the Office of SAFETY Act Implementation (“OSAI”) with the applications filed to date, OSAI has published numerous Frequently Asked Questions on its Web site as well as undertaken a substantial revision of the SAFETY Act Application Kit. The Department plans to publish a revised SAFETY Act Application Kit, which will account for the changes contained in this final rule and which will state with greater specificity the information required to properly evaluate a SAFETY Act application. For example, the Department agrees that some of the financial information requested in the original SAFETY Act Application Kit is not essential to the evaluation of every application. The Department, therefore, will limit the amount of financial information requested as part of the initial submission and to supplement the information as needed throughout the evaluation process.

The Department believes that the streamlining of the SAFETY Act Application Kit will result in further efficiency and time reductions. We anticipate making a revised SAFETY Act Application Kit available as soon as practicable.

C. Certifying “accuracy and completeness”

Two commenters expressed the opinion that it is unreasonable to require applicants to certify the application as “accurate and complete” under penalty of perjury when some of the questions require the applicant to provide answers on a “best guess” basis. In particular, the answers to the questions related to threat estimates, potential casualties, and potential casualty reductions were cited as questions whose answers may be essentially unknowable.

The Department agrees that it would be unreasonable to expect applicants to certify the application as “accurate and complete” under penalty of perjury when some of the questions require the applicant to provide answers on a “best guess” basis. In particular, the answers to the questions related to threat estimates, potential casualties, and potential casualty reductions were cited as questions whose answers may be essentially unknowable.

The Department agrees that it would be unreasonable to expect applicants to certify the accuracy of their speculative or predictive estimates of future events and risks. The language of the completeness certification is qualified, however, by the phrase “to the best of my knowledge and belief.” Since the applicant either knows or is able to obtain accurate factual information about the applicant’s anti-terrorism technology and business enterprise, the Department believes the application’s completeness certification is appropriate as to factual information and the application will so state. Conversely, since estimates are by definition not factual information, the Department’s position is that the completeness certification requires only that estimates be provided in good faith with a reasonable belief they are as accurate as possible at the time of submission. The Department will add this explanation as to estimates to the application form, and will consider all forms presented to date as incorporating this explanation.

D. Conditions on Designations

Two commenters took exception to the inclusion of limitations on SAFETY Act Designations (as such term is defined in 6 CFR 25.2) or Certifications (as such term is defined in 6 CFR 25.2), suggesting that the liability protections presented by the SAFETY Act potentially could be bypassed through a claim that such limitations imposed by the Department as a condition of SAFETY Act Designation were not met. The Department is aware of this concern and understands that undependable or uncertain liability protections would not have the desired effect of fostering the deployment of anti-terrorism technologies. Further, the Department is aware of the difficulty of crafting language for limitations that is not subject to multiple interpretations. As a general matter, the Department does not intend to impose conditions on SAFETY Act Designations and Certifications. If a question arises regarding the functionality of a technology, generally the Department will address and resolve that question in the course of the application process.

E. Significant Modification to a Qualified Anti-Terrorism Technology

Section 25.5(i) of the interim final rule has been the focus of significant attention, both by commenters and by members of Congress. That provision provided for automatic termination of SAFETY Act protection if a “significant modification” was made to a QATT, defined as a modification that could significantly reduce the technology’s safety or effectiveness, unless the Seller notified the Under Secretary and received approval of the modification. Several commenters have argued that the rule improperly suggests that a SAFETY Act Designation or Certification could terminate without notice if a “significant modification” is made to the QATT. Commenters have argued that, in hindsight, any routine, non-substantive or immaterial change in use, implementation, components, manufacturing process or other facet of a Technology might later be regarded as a “significant modification.” If such a change might be used later in litigation to invalidate SAFETY Act coverage retroactive to the time of the change, they argue, the value of a SAFETY Act Designation or Certification is minimal.

The American Bar Association, Public...
Contract Law Section commented, for instance, that: “the regulations should be clear that the designation cannot be stripped away after the fact by a claimant alleging a significant change * * *” Because the SAFETY Act covers all parties in the stream of commerce who rely on the designation and certification, it makes sense that their justifiable reliance not be undermined by retroactive effect back to the time of the change * * *” Other commenters were even more direct: “This requirement is misplaced in several respects and undermines the intent of the SAFETY Act to provide certainty and protection for those afforded coverage under the Act.”

“[T]he language of this provision is so broad that some unanticipated future change in operation, maintenance or methodology by a downstream user of the technology, totally outside the control of the QATT Seller, might ultimately be construed to terminate the Seller’s SAFETY Act coverage. This is particularly problematic for technologies involving technical services—almost every new application of these technologies will encounter unique circumstances and variations in operation, installation, implementation that, as a practical matter, might be construed to be ‘significant.’” Commenters indicated that section 25.5(i) was thus a “grave concern,” and that “it is essential that this provision be altered.”

The American Bar Association proposed regulatory language to address this issue, including the following: “The termination of the Designation will apply prospectively and will only affect products or services deployed after the DHS notice of termination * * *” In addition, commenters and certain members of Congress have raised concerns about the potential for changes to the statutory provision in § 863(d) of the SAFETY Act and the text of the section 25.5(i) of the interim final rule. Section 863(d) of the SAFETY Act provides that a SAFETY Act Certification is entitled to a presumption that the Government Contractor Defense applies, and specifies that a Certification may only terminate for one reason:

This presumption shall only be overcome by evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the course of the Secretary’s consideration of such technology under this subsection. § 863(d)(1)

Thus, the argument goes, because the statute specifies one and only one means to terminate a certification, the regulations cannot add a second route to termination through the “significant modification” provision.

The Department has carefully considered all of these comments and the legal arguments above. Section 25.5(i) of the interim final rule was intended to serve an important purpose—to provide the Department with knowledge of and the ability to address significant modifications that diminish the capability of a QATT. While the Department needs to preserve the intended function of this provision of the interim final rule, it agrees that changes to the provision are necessary to address the legal and policy concerns raised above.

The final rule eliminates language from section 25.5(i) of the interim final rule that could suggest that a Designation or Certification could terminate automatically and retroactively to the time of change and without notice, and replaces such language with a portion of the suggested language from the ABA commentary, and with procedures similar to those recommended by other commenters. To be clear, modifications that do not cause the QATT to be outside the scope of the QATT’s Designation or Certification will not adversely affect SAFETY Act coverage, nor are such modifications required to be notified to the Department. The final rule does not, however, eliminate the requirement that a Seller provide notice to the Department if the Seller intends to make, or has made, a modification that would cause the QATT to be outside the scope of a Designation or Certification.

The Department recognizes that many modifications to components, processes, use, implementation or other aspects of a technology occur from time to time during the life of a technology, and that many modifications either will have no consequence for the functionality of the Technology or will improve it. While certain proposed significant modifications should require review, many routine or non-significant modifications will not. The Department needs a rapid system for prospectively reviewing significant modifications that could reduce the effectiveness of a QATT. Such a system must recognize that routine changes may occur to components or processes that do not reduce the safety or effectiveness of the Technology.

This final rule modifies the procedure for Sellers to notify the Department of modifications or proposed modifications to a QATT and for the Department to respond quickly to such notifications with appropriate instructions for the Seller. Immaterial or routine modifications that are within the scope of the Designation will not require notice. It is important, however, and required, that the Department be informed of any significant modifications that the Seller makes or intends to make to a QATT. A significant modification is one that is outside the scope of a Designation. The Under Secretary will make the language of Designations and Certifications as precise as practicable under the circumstances to ensure that Sellers and other parties have fair notice of the scope of coverage, and in that regard the Department calls attention to the revisions in sections 25.6(e) and 25.9(f) of the final rule.

Whether notice to the Department is required for a change to a particular QATT will depend on the specific nature of the QATT and the terms of the Designation or Certification applicable to the QATT. If notice of a modification is required, review of the notice will also be undertaken in a reasonable time. If the Department does not take action in response to the notice, SAFETY Act coverage will be conclusively established. If the Department ultimately does not approve of the proposed changes, it will notify the Seller and may discuss possible remedial action to address the Department’s concerns or take other appropriate action in the discretion of the Under Secretary, as provided in section 25.6(l) of the final rule. In no event will a Designation terminate automatically or retroactively under this provision.

It is also important to recognize that the “significant modification” provisions may require notice by the Seller to the Department only when the modifications are made to a QATT by the Seller or are made to a QATT with the Seller’s knowledge and consent. The rule does not require that a Seller notify the Department of changes to a QATT made post-sale by an end-user of the QATT, and any such change by an end-user cannot result in loss of SAFETY Act protection for the Seller or others protected by the Seller’s Designation or Certification.

F. Exclusive Responsibility for Government Contractor Defense, Definitions of Fraud and Willful Misconduct

The Act is clear in allocating to the Secretary the exclusive responsibility for establishing the government contractor defense under section 861. The Act does not permit judicial review of the Secretary’s exercise of discretion in this context. When the Secretary determines that a Certification is appropriate, that decision creates a
rebuttable presumption that the government contractor defense applies. This presumption may only be rebutted “by clear and convincing evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Department during the course of the consideration of such Technology.” See section 25.8(b).

Two commenters expressed concern over the lack of a concrete standard of evidence for determining “fraud” or “willful misconduct.” One commenter specifically suggested adoption of the “clear and convincing evidence” standard from common-law civil fraud jurisprudence.

The Department agrees that the statutory presumption should only be overcome by evidence demonstrating an intentional effort to deceive the Department during the Certification process. This is the clear import of the statutory language and legislative history of the Act. Also, the traditional common law “clear and convincing evidence” standard is appropriate for evaluating a claim of fraud or willful misconduct in the SAFETY Act context.

G. Definition of “Act of Terrorism”

Two commenters expressed uncertainty concerning whether an act on foreign soil could be deemed an “Act of Terrorism” for purposes of the SAFETY Act. One commenter additionally requested clarification of the role of the Secretary in declaring whether a given event was or was not an “Act of Terrorism” for purposes of the SAFETY Act.

The definition of the term “Act of Terrorism” set forth in the SAFETY Act provides that any act meeting the requirements specified in the Act, as such requirements “are further defined and specified by the Secretary,” may be deemed an “Act of Terrorism.” In the interim rule, the Department presented its view that the term “Act of Terrorism” potentially encompasses acts that occur outside the territory of the United States. The Department stated that the basis for that view is “there is no geographic requirement in the definition: rather, an act that occurs anywhere may be covered if it causes harm to a person, property, or an entity in the United States.” The Department confirms its prior interpretation. The statutory requirements for what may be deemed an “Act of Terrorism” address the legality of the act in question, the harm such act caused, and whether instrumentality, weapons or other methods designed or intended “to cause mass destruction, injury or other loss to citizens or institutions of the United States” were employed. The statutory requirements are focused on the locus where harm was caused, the intent of the perpetrators and the victims of the particular act. See § 865(2)(B)(ii). The Department does not interpret the language of the Act to impose a geographical restriction for purposes of determining whether an act may be deemed an “Act of Terrorism.” In other words, the Act is concerned more with where effects of a terrorist act are felt rather than where on a map a particular act may be shown to have occurred. Accordingly, an act on foreign soil may indeed be deemed an “Act of Terrorism” for purposes of the SAFETY Act provided that it causes harm in the United States. The Department interprets “harm” in this context to include harm to financial interests. It is certainly possible that terrorist acts occurring outside the United States could be intended to cause, and may result in, devastating financial harm in the United States.

The focus of the “Act of Terrorism” definition is on where harm is realized is appropriate in light of the possibility that an Act of Terrorism may be the result of a series of actions occurring in multiple locations or that the locus of the terrorist act may not be readily discernible. This is especially the case with respect to acts of cyber terrorism.

H. Retroactive Designation

Five commenters found the distinction between “sales” and “deployments,” as expressed in the interim rule, to be confusing. The commenters expressed concern that similar deployments of identical QATTs might not be similarly protected, depending on when the deployment was made. In particular, failing to extend SAFETY Act liability protections retroactively may incentive Sellers to remove or nullify existing deployments, only to make identical new deployments at significant cost to the Seller and/or its customers.

The Department believes these commenters may have misunderstood the language of the interim rule. As part of each Designation or Certification, the Department will specify the earliest date that deployments of the QATT will be accorded the protections of that Designation or Certification. The Seller supplies the information concerning the earliest date the technology was deployed.

I. Bias Toward Product-Based Anti-Terrorism Technologies

Despite the assurances of the interim rule, particularly in the responses to comments on the Notice of Proposed Rulemaking, four commenters thought that the language of the interim rule and of the SAFETY Act Application Kit implicitly assumed that all anti-terrorism technologies would be product-based and not service-based or analysis-based.

To avoid any confusion on this issue, the definition of “Technology” set forth in this final rule clearly and unequivocally states that a Technology for SAFETY Act purposes includes “any product, equipment, service (including support services), device, or technology (including information technology) or any combination of the foregoing.” In particular, design services, consulting services, engineering services, software development services, software integration services, program management and integration services, threat assessments, vulnerability studies, and other analyses relevant to homeland security may each be deemed a Technology under the SAFETY Act. Corresponding changes will be incorporated into the revised SAFETY Act Application Kit. Further, this concern is not manifest in the operating history of the Act. Multiple anti-terrorism services have received SAFETY Act Designation to date.

J. Scope of Insurance Coverage

Several commenters suggested there is no reason for the insurance required to be purchased by Sellers pursuant to the Act to cover claims brought against the Seller’s supply and distribution chains since a plaintiff’s sole point of recovery with respect to claims implicating the SAFETY Act would be the Seller. Furthermore, commenters pointed out that insurance policies offering coverage for a Seller and the Seller’s contractors, subcontractors, suppliers, vendors and customers are not currently available on the open market.

The Department recognizes that an action for recovery of damages proximately caused by a QATT that arises out of an Act of Terrorism may only be properly brought against a Seller. Accordingly, the Department has specified, and will specify, in particular Designations, that the liability insurance required to be obtained by the Seller shall not be required to provide coverage for the Seller’s contractors, subcontractors, suppliers, vendors or customers.

K. Interactions With Public Law 85–804

Three commenters believed that the language in the interim rule concerning Public Law 85–804, and its relationship with the SAFETY Act, was unclear, especially in light of Executive Order 13286. In particular, the commenters...
sought clarification with respect to the circumstances in which both SAFETY Act Designation and indemnification under Public Law 85–804 might be available. One commenter suggested that DHS implement a mechanism for simultaneous SAFETY Act and Public Law 85–804 consideration in association with a procurement.

Commenters also expressed concern with the availability of Public Law 85–804 indemnification for technologies for which Sellers do not apply for (or receive) SAFETY Act Designation. They suggested that the phrase “any matter that has been, or could be, designated by the Secretary of Homeland Security as a Qualified Anti-Terrorism Technology” in Executive Order 13286 is a potential source of confusion and an obstacle to otherwise appropriate indemnification for Sellers who do not seek, and would not merit, Designation.

Section 73(b) of Executive Order 13286 revises Executive Order 10789 to state that no technology that has been, or could be, designated by a QATT, can be considered for indemnification under Public Law 85–804 (except by the Department of Defense) until “(i) the Secretary of Homeland Security has advised whether the use of the authority provided under [the SAFETY Act] would be appropriate, and (ii) the Director of the Office and Management and Budget has approved the exercise of authority under this order.”

The Department is sympathetic to the notion that separate processes in multiple agencies for Public Law 85–804 and SAFETY Act review could consume inordinate time and expense. The Department is supporting interagency efforts to find a solution to speed and ease the burden of both processes.

The Department acknowledges that some anti-terrorism technologies involve unusually hazardous risk, independent of an act of terrorism, and that indemnification under Public Law 85–804 might appropriately be made available under such circumstances. In those circumstances, both the SAFETY Act and Public Law 85–804 could be applicable to the same technology for different risks at the same time, and one process should not slow progress in the other. Executive Order 10789, as amended by section 73 of Executive Order 13286, allows for such a solution with the concurrence of the Director of the Office of Management and Budget.

Where appropriate, the Department will entertain letter requests for a “Notice of Inapplicability of SAFETY Act Designation,” which would allow entities to obtain a statement from the Department regarding the inappropriateness of SAFETY Act Designation for a particular technology in a particular context, outside of the established SAFETY Act application process. In this process, the Department expects that submitters will include sufficient information within their letter request to allow for a determination of inapplicability to be made. The Department will, however, reserve the right either to request additional information of the type included in the SAFETY Act application if it determines that the request does not adequately describe the Seller’s technology before a determination of applicability or inapplicability, as the case may be, can be made.

L. Prioritization of Evaluations

Three commenters noted the importance of an appropriate process for expediting SAFETY Act applications associated with government procurements that are ready to proceed and where the need for immediate indemnification is urgent and compelling. They also asked that the Department publish guidance describing how it plans to prioritize application reviews.

The Department will expedite the review of SAFETY Act applications that it deems particularly urgent and that involve government procurements and will publish guidance on how SAFETY Act applications and the government procurement process may best be aligned (See “Coordination with Government Procurements” below and section 25.6(g) of the rule).

M. Standards

Three commenters expressed concern about standards and suggested proposed changes to the interim rule in this area. The gist of these suggestions was to ensure that proprietary standards are not treated inappropriately by the Department, and that the Department not needlessly develop new standards in competition with existing, widely-accepted, proprietary standards. In addition, several commenters felt that adherence to certain existing standards, or to Federal certifications of various kinds, should be deemed conclusive evidence of compliance with certain SAFETY Act evaluation criteria.

The Department reiterates that it intends to protect proprietary and other protected information to the maximum extent possible. No copyrighted or otherwise protected intellectual property will be distributed by the Department without the express permission of the owner, unless the Department’s rights in that data have been acquired through some other manner. Where specific proprietary standards are relevant to the SAFETY Act evaluation process, the Department will advise applicants of the appropriate channels for obtaining copies of such standards.

The Department has to date and will continue to work closely with standard-setting organizations that have sought SAFETY Act protection for anti-terrorism standards. The Secretary has discretion to decide which standards are relevant with respect to the criteria for SAFETY Act Designation and Certification, and the Department remains open to the concept that a standard itself may constitute a QATT.

N. Expiration of Designations

Three commenters stated that Designations should not expire, or should at least have a minimum term of 10 years or more.

The Department notes that qualification for SAFETY Act coverage depends on a combination of the ability of the technology to be effective in a specific threat environment, the nature and cost of available insurance, and other factors, all of which are subject to change. At the same time, the Department is cognizant of the need for a guaranteed period of protection for successful SAFETY Act applicants to achieve the main goal of the Act, which is to facilitate the deployment of needed anti-terrorism technologies. Since the expiration of SAFETY Act Designation and Certification would impact only future sales of the subject QATT, the Department believes that mandatory reconsideration of Designations after five to eight years provides a fair balancing of public and private interests while providing the certainty required by Sellers. Sellers may apply for renewal up to two years prior to the expiration of their SAFETY Act Designation.

O. Appeal/Review of Decisions Regarding SAFETY Act Applications

Two commenters reiterated a request for an independent appeal or review process. The Department is aware of the complexity of the review process and has made and is making numerous allowances for exchange of information and concerns between evaluators and applicants at multiple points during the application process, to give the applicant further opportunity to provide supplemental information and address issues. The Department believes that this interactive process will provide sufficient recourse to applicants. The SAFETY Act is a discretionary authority accorded by Congress to the Secretary of Homeland Security to facilitate the commercialization and deployment of
needed anti-terrorism technologies. The exercise of that authority with respect to a particular technology requires that many discretionary judgments be made regarding the applicability of the SAFETY Act criteria to the technology and the weighting of the criteria in each case.

SAFETY Act protections are not a prerequisite for marketing any technology and therefore the absence of a grant of protection under the SAFETY Act will not prevent any person, firm or other entity from doing business. The Department also notes that a SAFETY Act Designation is not a “license required by law” within the meaning of the Administrative Procedure Act (APA), and thus is not covered by the APA. 5 U.S.C. 558(c).

P. Coordination With Government Procurements

The Department recognizes the need to align consideration of SAFETY Act applications from government procurement processes more closely. Accordingly, the final rule incorporates provisions that establish a flexible approach for such coordination. A government agency can seek a preliminary determination of SAFETY Act applicability, a “Pre-Qualification Designation Notice,” with respect to a technology to be procured. This notice would (i) establish the contractor to receive expedited review of a streamlined application for SAFETY Act coverage and (ii) most instances establish the presumption that the technology under consideration constitutes a QATT. If the technology in question has previously received Block Designation or Block Certification (as defined in 6 CFR 25.8), or the technology is based on established, well-defined specifications, the Department may indicate in DHS procurements, or make recommendations with respect to procurements of other public entities, that the contractor providing such technology will affirmatively receive Designation or Certification with respect to such technology, provided the contractor satisfies each other applicable requirement set forth in this final rule. In addition, the OSAI may expedite SAFETY Act review for technologies subject to ongoing procurement processes. The Department will on an on-going basis provide guidance for effectively coordinating government procurements (among Federal and non-Federal procurement officials) and consideration of SAFETY Act criteria. In addition, the Department may unilaterally determine that the subject of a procurement is eligible for SAFETY Act protections and give notice of such determination in connection with a government solicitation.

The final rule clarifies that a determination by the Department to designate, or not to designate, a particular technology as a QATT should not be viewed as a determination that the technology meets, or fails to meet, the requirements of any solicitation issued by a Federal government customer or a non-Federal government customer.

Q. Pre-Application Consultations

The Department regards the process by which an applicant seeks SAFETY Act coverage as necessarily interactive and cooperative. Accordingly, the final rule continues to provide that the Department and applicants may consult prior to the submission of SAFETY Act Application. These consultations will provide an opportunity for applicants to provide information about the technology under consideration, and will allow for the Department to address an applicant’s questions with respect to the application process and the criteria by which the Department evaluates the anti-terrorism technology. Prospective applicants may request such consultations through the pre-application process set forth in the SAFETY Act Application Kit. The confidentiality provisions in §25.10 are applicable to such consultations.

R. Developmental Testing and Evaluation Designations

The SAFETY Act provides the Secretary significant discretion in determining what may be designated a “Qualified Anti-Terrorism Technology.” Section 25.4 recognizes that there may be instances of certain anti-terrorism technologies being developed that could serve as an important homeland security resource but that require additional developmental testing and evaluation, e.g., a prototype of a particular technology that has undergone successful lab testing may require field testing or a controlled operational deployment to validate its safety and efficacy. This section provides that the system of litigation and risk management established by the SAFETY Act may be afforded to such technologies albeit with certain limitations and constraints that otherwise would not attach to Qualified Anti-Terrorism Technologies that are Designated pursuant to §25.4(a).

Developmental Testing and Evaluation (DT&E) Designations will facilitate the deployment of promising anti-terrorism technologies in the field either for test and evaluation purposes or in response to exigent circumstances, by providing, on a limited basis, the liability protections offered by the SAFETY Act. The limits on the protections offered by a DT&E Designation, as compared with a Designation issued pursuant to §25.4(a), are set forth in the final rule.

In general, DT&E Designations will include limitations on the use and deployment of the subject technology, remain terminable at-will by the Department should any concerns regarding the safety of technology come to light, and will have a limited term not to exceed a reasonable period for testing or evaluating the technology (presumptively not longer than 36 months). Further, the SAFETY Act liability protections associated with DT&E Designations will apply only to acts that occur during the period set forth in the particular DT&E Designation. The Department seeks further comment on this topic.

S. Seller’s Continuing Obligations With Respect to Maintaining Insurance

The Department received comments on insurance certification requirements. There is no change with respect to the obligation of the Seller to certify to the Department in writing that the insurance required to be maintained pursuant to a particular SAFETY Act Designation has been obtained. However, this rule modifies each Seller’s obligation to certify to the Department that the required insurance has been maintained, and to do so within 30 days of each anniversary of the issuance of their SAFETY Act Designation. A Seller’s obligation to certify on an annual basis that the required insurance has been maintained is now dependent upon the Under Secretary making a request for such an insurance certification from the Seller. In other words, following their initial insurance certification, Sellers will be obligated to certify that they have maintained the required insurance as set forth in their SAFETY Act Designation only upon the Department requesting such a certification. However, no change has been made to each Seller’s continuing obligation to advise the Department of any material change in the type or amount of liability insurance coverage that the Seller actually maintains.

T. Block Designations and Block Certifications

The Department has established a streamlined procedure for providing SAFETY Act coverage for qualified Sellers of certain categories of
technologies. Those Certifications or Designations are known as “Block Designations” or “Block Certifications.” Block Designations and Block Certifications may be issued at the Secretary’s discretion and are intended to recognize technology that meets the criteria for Designation as a Qualified Anti-Terrorism Technology and that is based on established performance standards or defined technical characteristics. Fundamentally, Block Designation or Block Certification will announce to potential Sellers of the subject QATT that the Department has determined that the QATT satisfies the technical criteria for either Certification or Designation and that no additional technical analysis will be required in evaluating applications from potential Sellers of that QATT. The terms of any such Block Designation or Block Certification will establish the procedures and conditions upon which an applicant may receive SAFETY Act coverage as a Seller of the subject technology. Applications from potential Sellers of a QATT that has received either Block Designation or Block Certification will receive expedited review and will not require submission of information concerning the technical merits of the underlying technology.

All Block Designations and Block Certifications will be published by the Department within ten days after the issuance thereof at http://www.safetyact.gov, and copies may also be obtained by mail by sending a request to: Directorate of Science and Technology, Office of SAFETY Act Implementation, Room 4320, Department of Homeland Security, Washington, DC 20528. Such publication will be coordinated to guard against the unauthorized disclosure of proprietary information. Any person, firm, or other entity that desires to qualify as a Seller of a QATT that is the subject of a Block Designation or Block Certification will be required to submit only those portions of the application referenced in § 25.6(a) that are specified in such Block Designation or Block Certification and otherwise to comply with terms of § 25.6(a) and the relevant Block Designation or Block Certification.

U. Reciprocal Waivers

Several commenters stated that reciprocal waivers of the type described in the SAFETY Act (reciprocal waivers of claims by the specified parties for losses sustained arising from an Act of Terrorism with respect to which a Qualified Anti-terrorist Technology is deployed) are not standard practice in most industries and that some parties may be unwilling to enter into such reciprocal agreements. The Department recognizes that the ability of the Seller to obtain the reciprocal waiver of claims with its contractors, subcontractors, suppliers, vendors, and customers, and contractors and subcontractors of the customers necessarily depends on action by parties other than the Seller and that it may not be possible to obtain such waivers in all circumstances. The Department’s view is that such waivers are not an absolute condition precedent or subsequent for the issuance, validity, effectiveness, duration, or applicability of a Designation because (1) obtaining such waivers often will be beyond the control of SAFETY Act applicants, (2) requiring all of such waivers as such a condition would thwart the intent of Congress in enacting the SAFETY Act by rendering the benefits of the SAFETY Act inapplicable in many otherwise appropriate situations, and (3) the consequences of failing to obtain the waivers are not specified in the Act. Accordingly, as was previously the case, this rule requires only a good faith effort by the Seller to secure these waivers.

V. Deference Due to Other Federal or State Regulatory or Procurement Officials

The Department has received multiple comments suggesting that the Department defer to the expertise of other Federal or state procurement officials in reviewing the technical criteria for SAFETY Act applications. The level of deference due to other governmental officials will depend on the nature of such officials’ review of the technology in question. In certain circumstances when qualified officials have determined specifically that a technology is appropriate for anti-terrorism purposes, such determinations may be accorded significant weight in the SAFETY Act application review process. In other circumstances, where a prior government determination was made for different purposes or by persons not qualified to address anti-terrorism threats, less weight will be given the prior determination. See § 25.4(b)(8).

III. Regulatory Requirements

A. Executive Order 12866

The Department has examined the economic implications of the final rule as required by Executive Order 12866. Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distributive impacts; and equity).

Executive Order 12866 classifies a rule as significant if it meets any one of a number of specified conditions, including: Having an annual effect on the economy of $100 million, adversely affecting a sector of the economy in a material way, adversely affecting competition, or adversely affecting jobs. A regulation is also considered a significant regulatory action if it raises novel legal or policy issues.

These matters were discussed in the interim rule and the Department received no comments on the economic analysis.

The Department concludes that the final rule is a significant regulatory action under the Executive Order because it will have a positive, material effect on public safety under section 3(f)(1) of Executive Order 12866, and it raises novel legal and policy issues under section 3(f)(4) of the Executive Order. The Department concludes, however, that the final rule does not meet the significance threshold of $100 million effect on the economy in any one year under section 3(f)(1), due to the relatively low estimated burden of applying for this technology program, the unknown number of Certifications and Designations that the Department will dispense, and the unknown probability of a terrorist attack that would have to occur in order for the protections put in place in the final rule to have a large impact on the public.

Need for the Regulation and Market Failure

The final rule implements the SAFETY Act and is intended to implement the provisions set forth in that Act. The Department believes the current development of anti-terrorism technologies has been slowed due to the potential liability risks associated with their development and eventual deployment. In a fully functioning insurance market, technology developers would be able to insure themselves against excessive liability risk; however, the terrorism risk insurance market appears to be in disequilibrium. The attacks of September 11 fundamentally changed the landscape of terrorism insurance. Congress, in the findings of the Terrorism Risk Insurance Act of 2002 (TRIA), concluded that temporary financial assistance in the insurance market is needed to “allow for a transitional period for the private markets to stabilize, resume pricing of such insurance, and build capacity to absorb any future losses.” Public Law...
107–237, 101(b)(2). This final rulemaking addresses a similar concern, to the extent that potential technology developers are unable to insure efficiently against large losses due to an ongoing reassessment of terrorism issues in insurance markets.

Even after a temporary insurance market adjustment, purely private terrorism risk insurance markets may exhibit negative externalities. Because the risk pool of any single insurer may not be large enough efficiently to spread and therefore insure against the risk of damages from a terrorist attack, and because the potential for excessive liability may render any terrorism insurance prohibitively expensive, society may suffer from less than optimal technological protection against terrorist attacks. The measures set forth in the final rule are designed to meet this goal; they will provide certain liability protection and consequently will increase the likelihood that businesses will pursue development and deployment of important technologies that may not be pursued without this protection.

Costs and Benefits to Technology Development Firms

Since this final rulemaking puts in place an additional voluntary option for technology developers, the expected direct net benefits to firms of this rulemaking will be positive; companies presumably will not choose to pursue the Designation of “Qualified Anti-Terrorism Technology” unless they believe it to be a profitable endeavor. The Department cannot predict with certainty the number of applicants for this program. An additional source of uncertainty is the reaction of the insurance market to this Designation. As mentioned above, insurance markets appear currently to be adjusting their strategy for terrorism risk, so little market information exists that would inform this estimate.

If a firm chooses to invest effort in pursuing SAFETY Act liability protection, the direct costs to that firm will be the time and money required to submit the required paperwork and other information to the Department. Only companies that choose to request this protection will incur paperwork costs in completing the application kit. The direct benefits to firms include lower potential losses from liability for terrorist attacks and, as a consequence, a lower burden from liability insurance for this type of technology. In this assessment, we were careful to consider only benefits and costs specifically due to the implementation of the final rule and not costs that would have been incurred by companies absent any rulemaking. The SAFETY Act requires the Sellers of the technology to obtain liability insurance “of such types and in such amounts” certified by the Secretary. The entire cost of insurance is not a cost specifically imposed by the proposed rulemaking, as companies in the course of good business practice routinely purchase insurance absent Federal requirements to do so. Any difference in the amount or price of insurance purchased as a result of the SAFETY Act would be a cost or benefit of the final rule for firms.

The language of the SAFETY Act clearly states that Sellers are not required to obtain liability insurance beyond the maximum amount of liability insurance reasonably available from private liability sources on the world market at prices and terms that will not unreasonably distort the sales price of the Seller’s Anti-Terrorism Technologies. We tentatively conclude, however, that this final rulemaking will impact both the prices and terms of liability insurance relative to the amount of insurance coverage absent the SAFETY Act. The probable effect of the final rule is to lower the quantity of liability coverage needed in order for a firm to protect itself from terrorism liability risks, which would be considered a benefit of the final rule to firms. This change will most likely be a reduction in demand that leads to a movement along the supply curve for technology firms already in this market; they probably will buy less liability coverage. This will have the effect of lowering the price per unit of coverage in this market.

The Department also expects, however, that this final rule will lead to greater market entry, which will generate benefits for technology firms but should also lead to a larger pool of potential products that will require insurance.

Costs and Benefits to Insurers

The Department has little information on the future structure of the terrorism risk insurance market, and how this final rule will affect that structure. As stated above, this type of intervention could serve to lower the demand for insurance in the current market, thus the static effect on the profitability of insurers is negative. The benefits of the lower insurance burden to technology firms would be considered a cost to insurers; the static changes to insurance coverage would cause a transfer of economic benefits from insurers to technology firms. On the other hand, this type of intervention should serve to increase the economic benefits of insurers by making some types of insurance products possible that would have been cost prohibitive for customers to purchase or insurers to design in the absence of this final rulemaking.

Costs and Benefits to the Public

The benefits to the public of this final rulemaking are very difficult to put in dollar value terms since the ultimate objective of the final rule is the development of new technologies that will help prevent or limit the damage from terrorist attacks. It is not possible to determine whether these technologies could help prevent large or small scale attacks, as the SAFETY Act applies to a vast range of technologies, including products, services, software, and other forms of intellectual property that could have a widespread impact. In qualitative terms, the SAFETY Act removes a great deal of the risk and uncertainty associated with product liability and in the process creates a powerful incentive that will help fuel the development of critically-needed anti-terrorism technologies. Additionally, we expect the SAFETY Act to reduce the research and development costs of these technologies.

The tradeoff, however, may be that a greater number of technologies may be developed and qualify for this program that have a lower average effectiveness against terrorist attacks than technologies currently on the market, or technologies that would be developed in the absence of this final rulemaking. In the absence of this rulemaking, strong liability discouragement implies that the fewer products that are deployed in support of anti-terrorist efforts may be especially effective, since profit maximizing firms will always choose to develop the technologies with the highest demand first. It is the tentative conclusion of the Department that liability discouragement in this market is currently too strong or prohibitive, for the reasons mentioned above. The Department tentatively concludes that the final rule will have positive net benefits to the public, since it serves to strike a better balance between consumer protection and technological development.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA) mandates that an agency conduct an RFA analysis when an agency is “required by section 553 * * *, or any other law, to publish general notice of proposed rulemaking for any proposed rule, or publishes a notice of proposed rulemaking involving the internal revenue laws of the United States * * *” 5 U.S.C.
603(a). The Regulatory Flexibility Act requires the Department to determine whether this final rulemaking will have a significant impact on a substantial number of small entities. Although we expect that many of the applicants for SAFETY Act protection are likely to meet the Small Business Administration’s criteria for being a small entity, we do not believe this final rulemaking will impose a significant financial impact on them. In fact, we believe the final rule will be a benefit to technology development businesses, especially small businesses, and present them with an attractive, voluntary option of pursuing a potentially profitable investment by reducing the amount of risk and uncertainty of lawsuits associated with developing anti-terrorist technology. The requirements of this final rulemaking will only be imposed on such businesses that voluntarily seek the liability protection of the SAFETY Act. If a company does not request that protection, the company will bear no cost from the final rule.

To the extent that demand for insurance falls, however, insurers may be adversely impacted by the final rule. The Department believes that eventual new entry into this market and further opportunities to insure against terrorism risk implies that the long-term impact of this final rulemaking on insurers is ambiguous but could very well be positive. We also expect that this final rulemaking will affect relatively few firms and relatively few insurers either positively or negatively, as this appears to be a specialized industry. Therefore, we certify this final rule will not have a significant impact on a substantial number of small entities.

C. Unfunded Mandates Reform Act of 1995

The final rule will not result in the expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year, and it will not significantly or uniquely affect small governments. Therefore, no actions were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

D. Executive Order 13132—Federalism

The Department of Homeland Security does not believe the final rule will have substantial direct effects on the States, on the relationship between the national government and the States, or on distribution of power and responsibilities among the various levels of government. States will, however, benefit from the final rule to the extent that they are purchasers of qualified anti-terrorism technologies.

E. Paperwork Reduction Act

The revised SAFETY Act Application Kit referenced above was released for comment with public notice published in the Federal Register on December 13, 2004, at 69 FR 72207. The SAFETY Act Application Kit may also be found at http://www.safetyact.gov. Concurrent with the publication of this final rule, the Department submitted a revised Paperwork Reduction Act package to the Office of Management and Budget (OMB) for review.

List of Subjects in 6 CFR Part 25

Business and industry, Insurance, Practice and procedure, Science and technology, Security measures.

For the reasons discussed in the preamble, 6 CFR part 25 is revised to read as follows:

PART 25—REGULATIONS TO SUPPORT ANTI-TERRORISM BY FOSTERING EFFECTIVE TECHNOLOGIES

§ 25.1 Purpose.
§ 25.2 Definitions.
§ 25.3 Delegation.
§ 25.4 Designation of Qualified Anti-Terrorism Technologies.
§ 25.5 Obligations of Seller.
§ 25.6 Procedures for Designation of Qualified Anti-Terrorism Technologies.
§ 25.7 Litigation Management.
§ 25.8 Government Contractor Defense.
§ 25.9 Procedures for Certification of Approved Products for Homeland Security.
§ 25.10 Confidentiality and Protection of Intellectual Property.


§ 25.1 Purpose.

This part implements the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, sections 441–444 of title 6, United States Code (the “SAFETY Act” or “the Act”).

§ 25.2 Definitions.

Act of Terrorism—The term “Act of Terrorism” means any act determined to have met the following requirements or such other requirements as defined and specified by the Secretary:

(1) Is unlawful;
(2) Causes harm, including financial harm, to a person, property, or entity, in the United States, or in the case of a domestic United States air carrier or a United States-flag vessel (or a vessel based principally in the United States on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), in or outside the United States; and
(3) Uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.

Certificate—The term “Certificate” means (unless the context requires otherwise) the certification issued pursuant to section 25.9 that a Qualified Anti-Terrorism Technology for which a Designation has been issued will perform as intended, conforms to the Seller’s specifications, and is safe for use as intended.

Contractor—The term “contractor” means any person, firm, or other entity with whom or with which a Seller has a contract or contractual arrangement relating to the manufacture, sale, use, or operation of anti-terrorism Technology for which a Designation is issued (regardless of whether such contract is entered into before or after the issuance of such Designation), including, without limitation, an independent laboratory or other entity engaged in testing or verifying the safety, utility, performance, or effectiveness of such Technology, or the conformity of such Technology to the Seller’s specifications.

Designation—The term “Designation” means the designation of a Qualified Anti-Terrorism Technology under the SAFETY Act issued by the Under Secretary under authority delegated to the Under Secretary by the Secretary of Homeland Security.

Loss—The term “loss” means death, bodily injury, or loss of or damage to property, including business interruption loss (which is a component of loss of or damage to property).

Noneconomic damages—The term “noneconomic damages” means damages for losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companionship, loss of consortium, hedonic damages, injury to reputation, and any other nonpecuniary losses.

Office of SAFETY Act Implementation—The term “Office of SAFETY Act Implementation” or “OSAI” means the office within the Department of Homeland Security’s Directorate of Science and Technology that assists with the implementation of the SAFETY Act. The responsibilities of the Office of SAFETY Act Implementation include, without limitation, preparing the SAFETY Act Application Kit, receiving and
facilitating the evaluation of applications, managing the SAFETY Act Web site and otherwise providing the public with information regarding the SAFETY Act and the application process.

Physical harm—The term “physical harm” as used in the Act and this part means any physical injury to the body, including an injury that caused, either temporarily or permanently, partial or total physical disability, incapacity or disfigurement. In no event shall physical harm include mental pain, anguish, or suffering, or fear of injury.

Qualified Anti-Terrorism Technology or QATT—The term “Qualified Anti-Terrorism Technology” or “QATT” means any Technology (including information technology) designed, developed, modified, procured, or sold for the purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, for which a Designation has been issued pursuant to this part.


SAFETY Act Application Kit —The term “SAFETY Act Application Kit” means the Application Kit containing the instructions and forms necessary to apply for Designation or Certification. The SAFETY Act Application Kit shall be published at http://www.safetyact.gov or made available in hard copy upon written request to: Directorate of Science and Technology, SAFETY Act/room 4320, Department of Homeland Security, Washington, DC 20528.

SAFETY Act Confidential Information—Any and all information and data voluntarily submitted to the Department under this part (including Applications, Pre-Applications, other forms, supporting documents and other materials relating to any of the foregoing, and responses to requests for additional information), including, but not limited to, inventions, devices, Technology, know-how, designs, copyrighted information, trade secrets, confidential business information, analyses, test and evaluation results, manuals, videotapes, contracts, letters, facsimile transmissions, electronic mail and other correspondence, financial information and projections, actuarial calculations, liability estimates, insurance quotations, and business and marketing plans. Notwithstanding the foregoing, “SAFETY Act Confidential Information” shall not include any information or data that is in the public domain or becomes part of the public domain by any means other than the violation of this section.

Secretary—the term “Secretary” means the Secretary of Homeland Security as established by section 102 of the Homeland Security Act of 2002.

Seller—the term “Seller” means any person, firm, or other entity that sells or otherwise provides Qualified Anti-Terrorism Technology to any customer(s) and to whom or to which (as appropriate) a Designation and/or Certification has been issued under this Part (unless the context requires otherwise).

Technology—the term “Technology” means any product, equipment, service (including support services), device, or technology (including information technology) or any combination of the foregoing. Design services, consulting services, engineering services, software development services, software integration services, threat assessments, vulnerability studies, and other analyses relevant to homeland security may be deemed a Technology under this part.

Under Secretary—the term “Under Secretary” means the Under Secretary for Science and Technology of the Department of Homeland Security.

§25.3 Delegation.

All of the Secretary’s responsibilities, powers, and functions under the SAFETY Act, except the authority to declare that an act is an Act of Terrorism for purposes of section 865(2) of the SAFETY Act, may be exercised by the Under Secretary for Science and Technology of the Department of Homeland Security or the Under Secretary’s designees.

§25.4 Designation of Qualified Anti-Terrorism Technologies.

(a) General. The Under Secretary may Designate as a Qualified Anti-Terrorism Technology for purposes of the protections under the system of litigation and risk management set forth in sections 441–444 of Title 6, United States Code, any qualifying Technology designed, developed, modified, provided or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause.

(b) Criteria to be Considered. (1) In determining whether to issue the Designation under paragraph (a) of this section, the Under Secretary may exercise discretion and judgment in considering the following criteria and evaluating the Technology:

(i) Prior United States Government use or demonstrated substantial utility and effectiveness.

(ii) Availability of the Technology for immediate deployment in public and private settings.

(iii) Existence of extraordinarily large or extraordinarily unquantifiable potential third party liability risk exposure to the Seller or other provider of such anti-terrorism Technology.

(iv) Substantial likelihood that such anti-terrorism Technology will not be deployed unless protections under the system of risk management provided under sections 441–444 of title 6, United States Code, are extended.

(v) Magnitude of risk exposure to the public if such anti-terrorism Technology is not deployed.

(vi) Evaluation of all scientific studies that can be feasibly conducted in order to assess the capability of the Technology to substantially reduce risks of harm.

(vii) Anti-terrorism Technology that would be effective in facilitating the defense against acts of terrorism, including Technologies that prevent, defeat or respond to such acts.

(viii) A determination made by Federal, State, or local officials, that the Technology is appropriate for the purpose of preventing, detecting, identifying or deterring acts of terrorism or limiting the harm such acts might otherwise cause.

(ix) Any other factor that the Under Secretary may consider to be relevant to the determination or to the homeland security of the United States.

(2) The Under Secretary has discretion to give greater weight to some factors over others, and the relative weighting of the various criteria may vary depending upon the particular Technology at issue and the threats that the Technology is designed to address. The Under Secretary may, in his discretion, determine that failure to meet a particular criterion justifies denial of an application under the SAFETY Act. However, the Under Secretary is not required to reject an application that fails to meet one or more of the criteria. The Under Secretary may conclude, after considering all of the relevant criteria and any other relevant factors, that a particular Technology merits Designation as a Qualified Anti-Terrorism Technology even if one or more particular criteria are not satisfied. The Under Secretary’s considerations will take into account evolving threats and conditions that give rise to the need for the anti-terrorism Technologies.

(c) Use of Standards. From time to time, the Under Secretary may develop,
issue, revise, adopt, and recommend technical standards for various technologies or components of anti-terrorism Technologies (“Adopted Standards”). In the case of Adopted Standards that are developed by the Department or that the Department has the right or license to reproduce, the Department will make such standards available to the public consistent with necessary protection of sensitive homeland security information. In the case of Adopted Standards that the Department does not have the right or license to reproduce, the Directorate of Science and Technology will publish a list and summaries of such standards and may publish information regarding the sources for obtaining copies of such standards. Compliance with any Adopted Standard or other technical standards that are applicable to a particular anti-terrorism Technology may be considered in determining whether a Technology will be Designated pursuant to paragraph (a) of this section. Depending on whether an Adopted Standard otherwise meets the criteria set forth in section 862 of the Homeland Security Act; 6 U.S.C. 441, the Adopted Standard itself may be deemed a Technology that may be Designated as a Qualified Anti-Terrorism Technology.

(d) Consideration of Substantial Equivalence. In considering the criteria in paragraph (b) of this section, or evaluating whether a particular anti-terrorism Technology complies with any Adopted Standard referenced in paragraph (c) of this section, the Under Secretary may consider evidence that the Technology is substantially equivalent to other Technologies (“Predicate Technologies”) that previously have been Designated as Qualified Anti-Terrorism Technologies under the SAFETY Act. A Technology may be deemed to be substantially equivalent to a Predicate Technology if:

(1) It has the same intended use as the Predicate Technology; and
(2) It has the same or substantially similar performance or technological characteristics as the Predicate Technology.

(e) Pre-Application Consultations. To the extent that he deems it to be appropriate, the Under Secretary may consult with prospective and current SAFETY Act applicants regarding their particular anti-terrorism Technologies. Prospective applicants may request such consultations through the Office of SAFETY Act Implementation. The confidential provisions in §25.10 shall be applicable to such consultations.

(f) Developmental Testing & Evaluation (DT&E) Designations. With respect to any Technology that is being developed, tested, evaluated, modified or is otherwise being prepared for deployment for the purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, the Under Secretary may Designate such Technology as a Qualified Anti-Terrorism Technology and make such Technology eligible for the protections under the system of litigation and risk management set forth in sections 441–444 of title 6, United States Code. A Designation made pursuant to this paragraph shall be referred to as a "DT&E Designation," and shall confer all of the rights, privileges and obligations that accompany Designations made pursuant to paragraph (a) of this section except as modified by the terms of this paragraph or the terms of the particular DT&E Designation. The intent of this paragraph is to make eligible for SAFETY Act protections qualifying Technologies that are undergoing testing and evaluation and that may need to be deployed in the field either for developmental testing and evaluation purposes or on an emergency basis, including during a period of heightened risk. DT&E Designations shall describe the subject Technology (in such detail as the Under Secretary deems to be appropriate); identify the Seller of the subject Technology; be limited to the period of time set forth in the applicable DT&E Designation, which in no instance shall exceed a reasonable period for testing or evaluating the Technology (presumptively not longer than 36 months); be terminable by the Under Secretary at any time upon notice to the Seller; be subject to the limitations on the use or deployment of the QATT set forth in the DT&E Designation; and be subject to such other limitations as established by the Under Secretary. The protections associated with a DT&E Designation shall apply only during the period specified in the applicable DT&E Designation. Consent of the Seller of a QATT Designated pursuant to this paragraph will be a condition precedent to the establishment of any deployment or use condition and any other obligation established by the Under Secretary pursuant to this paragraph. Those seeking a DT&E Designation for a QATT pursuant to this paragraph (f) shall follow the procedures for DT&E Designations set forth in the SAFETY Act Application Kit.

§25.5 Obligations of Seller.

(a) Liability Insurance Required. The Seller shall obtain liability insurance of such types and in such amounts as shall be required in the applicable Designation, which shall be the amounts and types certified by the Under Secretary to satisfy otherwise compensable third-party claims arising out of, relating to, or resulting from an Act of Terrorism when Qualified Anti-Terrorism Technologies have been deployed in defense against, response to, or recovery from, such act. The Under Secretary may request at any time that the Seller of a Qualified Anti-Terrorism Technology submit any information that would:

(1) Assist in determining the amount of liability insurance required; or
(2) Show that the Seller or any other provider of Qualified Anti-Terrorism Technology otherwise has met all of the requirements of this section.

(b) Amount of Liability Insurance.

(1) The Under Secretary may determine the appropriate amounts and types of liability insurance that the Seller will be required to obtain and maintain based on criteria he may establish to satisfy compensable third-party claims arising from, relating to or resulting from an Act of Terrorism. In determining the amount of liability insurance required, the Under Secretary may consider any factor, including, but not limited to, the following:

(i) The particular Technology at issue;
(ii) The amount of liability insurance the Seller maintained prior to application;
(iii) The amount of liability insurance maintained by the Seller for other Technologies or for the Seller’s business as a whole;
(iv) The amount of liability insurance typically maintained by Sellers of comparable Technologies;
(v) Information regarding the amount of liability insurance offered on the world market;
(vi) Data and history regarding mass casualty losses;
(vii) The intended use of the Technology; and
(viii) The possible effects of the cost of insurance on the price of the product, and the possible consequences thereof for development, production, or deployment of the Technology.

(2) In determining the appropriate amounts and types of insurance that a particular Seller is obligated to carry, the Under Secretary may not require any type of insurance or any amount of insurance that is not available on the world market, and may not require any type or amount of insurance that would
(c) Scope of Coverage. (1) Liability insurance required to be obtained pursuant to this section shall, in addition to the Seller, protect the following, to the extent of their potential liability for involvement in the manufacture, qualification, sale, use, or operation of Qualified Anti-Terrorism Technologies deployed in defense against, response to, or recovery from, an Act of Terrorism:

(i) Contractors, subcontractors, suppliers, vendors and customers of the Seller.

(ii) Contractors, subcontractors, suppliers, and vendors of the customer.

(2) Notwithstanding the foregoing, in appropriate instances the Under Secretary will specify in a particular Designation that, consistent with the Department’s interpretation of the SAFETY Act, an action for the recovery of damages proximately caused by a Qualified Anti-Terrorism Technology that arises out of, relates to, or results from an Act of Terrorism may properly be brought only against the Seller and, accordingly, the liability insurance required to be obtained pursuant to this section shall be required to protect only the Seller.

(d) Third Party Claims. To the extent available pursuant to the SAFETY Act, liability insurance required to be obtained pursuant to this section shall provide coverage against third party claims arising out of, relating to, or resulting from an Act of Terrorism when the applicable Qualified Anti-Terrorism Technologies have been deployed in defense against, response to, or recovery from such act.

(e) Reciprocal Waiver of Claims. The Seller shall enter into a reciprocal waiver of claims with its contractors, subcontractors, suppliers, vendors, and customers, and contractors and subcontractors of the customers, involved in the manufacture, sale, use, or operation of Qualified Anti-Terrorism Technologies, under which each party to the waiver agrees to be responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity resulting from an Act of Terrorism when Qualified Anti-Terrorism Technologies have been deployed in defense against, response to, or recovery from such act. Notwithstanding the foregoing, provided that the Seller has used diligent efforts in good faith to obtain all required reciprocal waivers, obtaining such waivers shall not be a condition precedent or subsequent for, nor shall the failure to obtain one or more of such waivers adversely affect, the issuance, validity, effectiveness, duration, or applicability of a Designation or a Certification. Nothing in this paragraph shall be interpreted to render the failure to obtain one or more of such waivers a condition precedent or subsequent for the issuance, validity, effectiveness, duration, or applicability of a Designation or a Certification.

(f) Information to be Submitted by the Seller. As part of any application for a Designation, the Seller shall provide all information that may be requested by the Under Secretary or his designee, regarding the Seller’s liability insurance coverage applicable to third-party claims arising out of, relating to, or resulting from an Act of Terrorism when the Seller’s Qualified Anti-Terrorism Technology has been deployed in defense against, response to, or recovery from such act, including:

(1) Names of insurance companies, policy numbers, and expiration dates;

(2) A description of the types and nature of such insurance (including the extent to which the Seller is self-insured or intends to self-insure);

(3) Dollar limits per occurrence and annually of such insurance, including any applicable sublimits;

(4) Deductibles or self-insured retentions, if any, that are applicable;

(5) Any relevant exclusions from coverage under such policies or other factors that would affect the amount of insurance proceeds that would be available to satisfy third party claims arising out of, relating to, or resulting from an Act of Terrorism;

(6) The price for such insurance, if available, and the per-unit amount or percentage of such price directly related to liability coverage for the Seller’s Qualified Anti-Terrorism Technology deployed in defense against, or response to, or recovery from an Act of Terrorism;

(7) Where applicable, whether the liability insurance, in addition to the Seller, protects contractors, subcontractors, suppliers, vendors and customers of the Seller and contractors, subcontractors, suppliers, vendors and customers of the customer to the extent of their potential liability for involvement in the manufacture, qualification, sale, use or operation of Qualified Anti-Terrorism Technologies deployed in defense against, response to, or recovery from an Act of Terrorism; and

(8) Any limitations on such liability insurance.

(g) Under Secretary’s Certification. For each Qualified Anti-Terrorism Technology, the Under Secretary shall certify the amount of liability insurance the Seller is required to carry pursuant to section 443(a) of title 6, United States Code, and paragraphs (a), (b), and (c) of this section. The Under Secretary shall include the insurance certification under this section as a part of the applicable Designation. The insurance certification may specify a period of time for which such insurance certification will apply. The Seller of a Qualified Anti-Terrorism Technology may at any time petition the Under Secretary for a revision of the insurance certification under this section, and the Under Secretary may revise such insurance certification in response to such a petition. The Under Secretary may at any time request information from the Seller regarding the insurance carried by the Seller or the amount of insurance available to the Seller.

(h) Seller’s Continuing Obligations. Within 30 days after the Under Secretary’s insurance certification required by paragraph (g) of this section, the Seller shall certify to the Under Secretary in writing that the Seller has obtained the required insurance. Within 30 days of each anniversary of the issuance of a Designation or at any other time as he may determine, the Under Secretary may require, by written notice to the Seller, that the Seller certify to the Under Secretary in writing that the Seller has maintained the required insurance. The Under Secretary may terminate a Designation if the Seller fails to provide any of the insurance certifications required by this paragraph (h) or provides a false certification.

§ 25.6 Procedures for Designation of Qualified Anti-Terrorism Technologies.

(a) Application Procedure. Any person, firm or other entity seeking a Designation shall submit an application to the Under Secretary or such other official as may be named from time to time by the Under Secretary. Such applications shall be submitted according to the procedures set forth in and using the appropriate forms contained in the SAFETY Act Application Kit prescribed by the Under Secretary, which shall be made available at http://www.safetyact.gov and by mail upon written request to: Directorate of Science and Technology, SAFETY Act/room 4320, Department of Homeland Security, Washington, DC 20528. The burden is on the applicant to make timely submission of all relevant data requested in the SAFETY Act Application Kit to substantiate an application for Designation. An applicant may withdraw a submitted application at any time and for any reason by making a written request for withdrawal with the Department. Withdrawal of a SAFETY Act
application shall have no prejudicial effect on any other application.

(b) Initial Notification. Within 30 days after receipt of an application for a Designation, the Under Secretary his designee shall notify the applicant in writing that:

(1) The application is complete and will be reviewed and evaluated; or
(2) That the application is incomplete, in which case the missing or incomplete parts will be specified.

(c) Review Process. (1) The Under Secretary or his designee will review each complete application and any included supporting materials. In performing this function, the Under Secretary or his designee may but is not required to:

(i) Request additional information from the Seller;
(ii) Meet with representatives of the Seller;
(iii) Consult with, and rely upon the expertise of, any other Federal or non-Federal entity;
(iv) Perform studies or analyses of the subject Technology or the insurance market for such Technology; and
(v) Seek information from insurers regarding the availability of insurance for such Technology.

(2) For Technologies with which a Federal, State, or local government agency already has substantial experience or data (through the procurement process or through prior use or review), the review may rely in part upon such prior experience and, thus, may be expedited. The Under Secretary may consider any scientific studies, testing, field studies, or other experience with the Technology that he deems appropriate and that are available or can be feasibly conducted or obtained, including test results produced by an independent laboratory or other entity engaged to test or verify the safety, utility, performance, in order to assess the effectiveness of the Technology or the capability of the Technology to substantially reduce risks of harm. Such studies may, in the Under Secretary’s discretion, include, without limitation:

(i) Public source studies;
(ii) Classified and otherwise confidential studies;
(iii) Studies, tests, or other performance records or data provided by or available to the producer of the specific Technology; and
(iv) Proprietary studies that are available to the Under Secretary.

(3) In considering whether or the extent to which it is feasible to defer a decision on a Designation until additional scientific studies can be conducted on a particular Technology, the Under Secretary will bring to bear his expertise concerning the protection of the security of the United States and will consider the urgency of the need for the Technology.

(d) Action by the Under Secretary. Within 90 days of notification to the Seller that an application for a Designation is complete in accordance with paragraph (b)(1) of this section, the Under Secretary shall take one of the following actions:

(1) Approve the application and issue an appropriate Designation to the applicant for the Technology, which shall include the insurance certification required by § 25.5(h) of this Part;
(2) Notify the applicant in writing that the Technology is potentially eligible for a Designation, but that additional specified information is needed before a decision may be reached; or
(3) Deny the application, and notify the applicant in writing of such decision. The Under Secretary may extend the 90-day time period for up to 45 days upon notice to the Seller. The Under Secretary is not required to provide a reason or cause for such extension. The Under Secretary’s decision shall be final and not subject to review, except at the discretion of the Under Secretary.

(e) Content of Designation. (1) A Designation shall:

(i) Describe the Qualified Anti-Terrorism Technology (in such detail as the Under Secretary deems to be appropriate);
(ii) Identify the Seller(s) of the Qualified Anti-Terrorism Technology;
(iii) Specify the earliest date of sale of the Qualified Anti-Terrorism Technology to which the Designation shall apply (which shall be determined by the Under Secretary in his discretion, and may be prior to, but shall not be later than, the effective date of the Designation);
(iv) Set forth the insurance certification required by § 25.5(g); and
(v) To the extent practicable, include such standards, specifications, requirements, performance criteria, limitations, or other information as the Department in its sole and unreviewable discretion may deem appropriate.

(2) The Designation may, but need not, specify other entities that are required to be covered by the liability insurance required to be purchased by the Seller. The failure to specify a covered person, firm, or other entity in a Designation will not preclude the application or applicability of the Act’s protections to that person, firm, or other entity.

(f) Term of Designation; Renewal. A Designation shall be valid and effective for a term of five to eight years (as determined by the Under Secretary) commencing on the date of issuance, and the protections conferred by the Designation shall continue in full force and effect indefinitely to all sales of Qualified Anti-Terrorism Technologies covered by the Designation. At any time within two years prior to the expiration of the term of the Designation, the Seller may apply for renewal of the Designation. The Under Secretary shall make the application form for renewal available at http://www.safetyact.gov and by mail upon request sent to:

Directorate of Science and Technology,

(g) Government Procurements. (1) Overview. The Under Secretary may coordinate the review of a Technology for SAFETY Act purposes in connection with a Federal, State, or local government agency procurement of an anti-terrorism Technology in any manner he deems appropriate and consistent with the Act and other applicable law.

A determination by the Under Secretary to issue a Designation, or not to issue a Designation for a particular Technology as a QATT is not a determination that the Technology meets, or fails to meet, the requirements of any solicitation issued by any Federal government customer or non-Federal government customer. Determinations by the Under Secretary with respect to whether to issue a Designation for Technologies submitted for his review shall be based on the factors identified in § 25.4(b).

(2) Procedure. Any Federal, State, or local government agency that engages in or is planning to engage in the procurement of a Technology that potentially qualifies as a Qualified Anti-terrorism Technology, through the use of a solicitation of proposals or otherwise, may request that the Under Secretary issue a notice stating that the Technology to be procured either affirmatively or presumptively satisfies the technical criteria necessary to be deemed a Qualified Anti-Terrorism Technology (a “Pre-Qualification Designation Notice”). The Pre-Qualification Designation Notice will provide that the vendor(s) chosen to provide the Technology (the “Selected Vendor(s)”), upon submitting an application for SAFETY Act Designation will: Receive expedited review of their application for Designation; either affirmatively or presumptively (as the case may be) be deemed to have satisfied the technical criteria for SAFETY Act Designation with respect to the Technology identified in the Pre-Qualification Designation Notice; and be
authorized to submit a streamlined application as set forth in the Pre-Qualification Designation Notice. In instances in which the subject procurement involves Technology with respect to which a Block Designation or Block Certification has been issued, the Department may determine that the vendor providing such Technology will affirmatively receive Designation or Certification with respect to such Technology, provided the vendor satisfies each other applicable requirement for Designation or Certification. Government agencies seeking a Pre-Qualification Designation Notice shall submit a written request using the “Procurement Pre-Qualification Request” form prescribed by the Under Secretary and made available at http://www.safetyact.gov and by mail upon request sent to: Directorate of Science and Technology, SAFETY Act/room 4320, Department of Homeland Security, Washington, DC 20528.

3. Actions. Within 60 days after the receipt of a complete Procurement Pre-Qualification Request, the Under Secretary shall take one of the following actions:

(i) Approve the Procurement Pre-Qualification Request and issue an appropriate Pre-Qualification Designation Notice to the requesting agency that it may include in the government contract or in the solicitation materials, as appropriate; or

(ii) Notify the requesting agency in writing that the relevant procurement is potentially eligible for a Pre-Qualification Designation Notice, but that additional information is needed before a decision may be reached; or

(iii) Deny the Procurement Pre-Qualification Request and notify the requesting agency in writing of such decision, including the reasons for such denial.

4. Contents of Notice. A Pre-Qualification Designation Notice shall contain, at a minimum, the following:

(i) A detailed description of and detailed specifications for the Technology to which the Pre-Qualification Designation Notice applies, which may incorporate by reference all or part of the procurement solicitation documents issued or to be issued by the requesting agency;

(ii) A statement that the Technology to which the Pre-Qualification Designation Notice applies satisfies the technical criteria to be deemed a Qualified Anti-Terrorism Technology and that the Selected Vendor(s) may presumptively or will qualify for the issuance of a Designation or Block Certification with respect to such Technology upon compliance with the terms and conditions set forth in such Pre-Qualification Designation Notice and the approval of the streamlined application;

(iii) A list of the portions of the application referenced in §25.6(a) that the Selected Vendor(s) must complete and submit to the Department in order to obtain Designation and the appropriate period of time for such submission;

(iv) The period of time within which the Under Secretary will take action upon such submission;

(v) The date of expiration of such Pre-Qualification Designation Notice; and

(vi) Any other terms or conditions that the Under Secretary deems to be appropriate in his discretion.

5. Review of Completed Applications. The application for Designation from the Selected Vendor(s) shall be considered, processed, and acted upon in accordance with the procedures set forth in §25.6 (which shall be deemed to be modified by the terms and conditions set forth in the applicable Pre-Qualification Designation Notice). However, the review and evaluation of the Technology to be procured from the Selected Vendors(s), in relation to the criteria set forth in §25.4(b), shall ordinarily consist of a validation that the Technology complies with the detailed description of and detailed specifications for the Technology set forth in the applicable Pre-Qualification Designation Notice.

(h) Block Designations. (1) From time to time, the Under Secretary, in response to an application submitted pursuant to §25.6(a) or upon his own initiative, may issue a Designation that is applicable to any person, firm, or other entity that is a qualified Seller of the QATT described in such Designation (a “Block Designation”). A Block Designation will be issued only for Technology that relies on established performance standards or defined technical characteristics. All Block Designations shall be published by the Department within ten days after the issuance thereof at http://www.safetyact.gov, and copies may also be obtained by mail by sending a request to: Directorate of Science and Technology, SAFETY Act/room 4320, Department of Homeland Security, Washington, DC 20528. Any person, firm, or other entity that desires to qualify as a Seller of a QATT that has received a Block Designation shall complete only such portions of the application referenced in §25.6(a) as are specified in such Block Designation and shall submit an application to the Department in accordance with §25.6(a) and the terms of the Block Designation. Applicants seeking to be qualified Sellers of a QATT pursuant to a Block Designation will receive expedited review of their applications and shall not be required to provide information with respect to the technical merits of the QATT that has received Block Designation. Within 60 days (or such other period of time as may be specified in the applicable Block Designation) after the receipt by the Department of a complete application, the Under Secretary shall take one of the following actions:

(i) Approve the application and notify the applicant in writing of such approval, which notification shall include the certification required by §25.5(g); or

(ii) Deny the application, and notify the applicant in writing of such decision, including the reasons for such denial.

(2) If the application is approved, commencing on the date of such approval the applicant shall be deemed to be a Seller under the applicable Block Designation for all purposes under the SAFETY Act, this part, and such Block Designation. A Block Designation shall be valid and effective for a term of five to eight years (as determined by the Under Secretary in his discretion) commencing on the date of issuance, and may be renewed or extended by the Under Secretary at his own initiative or in response to an application for renewal submitted by a qualified Seller under such Block Designation in accordance with §25.6(h). Except as otherwise specifically provided in this paragraph, a Block Designation shall be deemed to be a Designation for all purposes under the SAFETY Act and this part.

(i) Other Bases for Expedited Review of Applications. The Under Secretary may identify other categories or types of Technologies for which expedited processing may be granted. For example, the Under Secretary may conduct expedited processing for applications addressing a particular threat or for particular types of anti-terrorism Technologies. The Under Secretary shall notify the public of any such opportunities for expedited processing by publishing such notice in the Federal Register.

(j) Transfer of Designation. Except as may be restricted by the terms and conditions of a Designation, any Designation may be transferred and assigned to any other person, firm, or other entity to which the Seller transfers and assigns all right, title, and interest in and to the Technology covered by the Designation, including all intellectual property rights therein (or, if the Seller is a licensee of the Technology, to any
person, firm, or other entity to which such Seller transfers all of its right, title, and interest in and to the applicable license agreement). Such transfer and assignment of a Designation will not be effective unless and until the Under Secretary is notified in writing of the transfer using the “Application for Transfer of Designation” form issued by the Under Secretary (the Under Secretary shall make this application form available at http://www.safetyact.gov and by mail by written request sent to: Directorate of Science and Technology, SAFETY Act/ room 4320, Department of Homeland Security, Washington, DC 20528). Upon the effectiveness of such transfer and assignment, the transferee will be deemed to be a Seller in the place and stead of the transferor with respect to the applicable Technology for all purposes under the SAFETY Act, this part, and the transferred Designation. The transferred Designation will continue to apply to the transferor with respect to all transactions and occurrences that occurred through the time at which the transfer and assignment of the Designation became effective, as specified in the applicable Application for Transfer of Designation.

(k) Application of Designation to Licensees. Except as may be restricted by the terms and conditions of a Designation, any Designation shall apply to any other person, firm, or other entity to which the Seller licenses (exclusively or nonexclusively) the right to manufacture, use, or sell the Technology, in the same manner and to the same extent that such Designation applies to the Seller, effective as of the date of commencement of the license, provided that the Seller notifies the Under Secretary of such license by submitting, within 30 days after such date of commencement, a “Notice of License of Qualified Anti-terrorism Technology” form issued by the Under Secretary. The Under Secretary shall make this form available at http://www.safetyact.gov and by mail upon request sent to: Directorate of Science and Technology, SAFETY Act/ room 4320, Department of Homeland Security, Washington, DC 20528. Such notification shall not be required for any licensee listed as a Seller on the applicable Designation.

(l) Significant Modification of Qualified Anti-terrorism Technologies. (1) The Department recognizes that Qualified Anti-Terrorism Technologies may routinely undergo changes or modifications in their manufacturing, materials, installation, implementation, operating processes, component assembly, or in other respects from time to time. When a Seller makes routine changes or modifications to a Qualified Anti-Terrorism Technology, such that the QATT remains within the scope of the description set forth in the applicable Designation or Certification, the Seller shall not be required to provide notice under this subsection, and the changes or modifications shall not adversely affect the force or effect of the Seller’s QATT Designation or Certification.

(2) A Seller shall promptly notify the Department and provide details of any change or modification to a QATT that causes the QATT no longer to be within the scope of the Designation or Certification by submitting to the Department a completed “Notice of Modification to Qualified Anti-Terrorism Technology” form issued by the Under Secretary (a “Modification Notice”). A Seller is not required to notify the Department of any change or modification of a particular Qualified Anti-Terrorism Technology that is made post-sale by a purchaser unless the Seller has consented expressly to the modification. The Under Secretary shall make an appropriate form available at http://www.safetyact.gov and by mail upon request sent to: Directorate of Science and Technology, SAFETY Act/ room 4320, Department of Homeland Security, Washington, DC 20528. The Department will promptly acknowledge receipt of a Modification Notice by providing the relevant Seller with written notice to that effect. Within 60 days of the receipt of a Modification Notice, the Under Secretary may, in his sole and unreviewable discretion:

(i) Inform the submitting Seller that the QATT as changed or modified is consistent with, and is not outside the scope of, the Seller’s Designation or Certification;

(ii) Issue to the Seller a modified Designation or Certification incorporating some or all of the notified changes or modifications;

(iii) Seek further information regarding the changes or modifications and temporarily suspend the 60-day period of review;

(iv) Inform the submitting Seller that the changes or modifications might cause the QATT as changed or modified to be outside the scope of the Seller’s Designation or Certification, and require further review and consideration by the Department;

(v) Inform the submitting Seller that the QATT as changed or modified is outside the scope of the subject Seller’s Designation or Certification, and require that the QATT be brought back into conformance with the Seller’s Designation or Certification; or

(vi) If the Seller fails to bring the subject QATT into conformance in accordance with the Under Secretary’s direction pursuant to paragraph (l)(2)(v) of this section, issue a public notice stating that the QATT as changed or modified is outside the scope of the submitting Seller’s Designation or Certification and, consequentially, that such Designation or Certification is not applicable to the QATT as changed or modified. If the Under Secretary does not take one or more of such actions within the 60-day period following the Department’s receipt of a Seller’s Modification Notice, the changes or modifications identified in the Modification Notice will be deemed to be approved by the Under Secretary and the QATT, as changed or modified, will be conclusively established to be within the scope of the description of the QATT in the Seller’s Designation or Certification.

(3) Notwithstanding anything to the contrary herein, a Seller’s original QATT Designation or Certification will continue in full force and effect in accordance with its terms unless modified, suspended, or terminated by the Under Secretary in his discretion, including during the pendency of the review of the Seller’s Modification Notice. In no event will any SAFETY Act Designation or Certification terminate automatically or retroactively under this section. A Seller is not required to notify the Under Secretary of any change or modification that is made post-sale by a purchaser or end-user of the QATT without the Seller’s consent, but the Under Secretary may, in appropriate circumstances, require an end-user to provide periodic reports on modifications or permit inspections or audits.

§ 25.7 Litigation Management

(a) Liability for all claims against a Seller arising out of, relating to, or resulting from an Act of Terrorism when such Seller’s Qualified Anti-Terrorism Technology has been deployed in defense against, response to, or recovery from such act and such claims result or may result in loss to the Seller shall not be in an amount greater than the limits of liability insurance coverage required to be maintained by the Seller under this section or as specified in the applicable Designation.

(b) In addition, in any action for damages brought under section 442 of Title 6, United States Code:

(1) No punitive damages intended to punish or deter, exemplary damages, or other damages not intended to compensate a plaintiff for actual losses
may be awarded. nor shall any party be
liable for interest prior to the judgment;
(2) Noneconomic damages may be
awarded against a defendant only in an
amount directly proportional to the
percentage of responsibility of such
defendant for the harm to the plaintiff,
and no plaintiff may recover
noneconomic damages unless the
plaintiff suffered physical harm; and
(3) Any recovery by a plaintiff shall be
reduced by the amount of collateral
source compensation, if any, that the
plaintiff has received or is entitled to
receive as a result of such Acts of
Terrorism that result or may result in
loss to the Seller.
(c) Without prejudice to the authority of the
Under Secretary to terminate a
Designation pursuant to paragraph (h) of
§ 25.6, the liability limitations and
reductions set forth in this section shall
apply in perpetuity to all sales or
deployments of a Qualified Anti-
Terrorism Technology in defense
against, response to, or recovery from any
Act that occurs on or after the
effective date of the
Designation applicable to such
Qualified Anti-Terrorism Technology,
regardless of whether any liability
insurance coverage required to be
obtained by the Seller is actually
obtained or maintained or not, provided
that the sale of such Qualified Anti-
Terrorism Technology was
consummated by the Seller on or after
the earliest date of sale of such
Qualified Anti-Terrorism Technology
specified in such Designation and prior
to the earlier of the expiration or
termination of such Designation.
(d) There shall exist only one cause of
action for loss of property, personal
injury, or death for performance or non-
performance of the Seller’s Qualified
Anti-Terrorism Technology in relation
to an Act of Terrorism. Such cause of
action may be brought only against the
Seller of the Qualified Anti-Terrorism
Technology and may not be brought
against the buyers, the buyers’
contractors, or downstream users of the
Technology, the Seller’s suppliers or
contractors, or any other person or
terity. In addition, such cause of action
must be brought in the appropriate
district court of the United States.

§ 25.8 Government Contractor Defense

(a) Criteria for Certification. The
Under Secretary may issue a
Certification for a Qualified Anti-
Terrorism Technology as an Approved
Product for Homeland Security for
purposes of establishing a rebuttable
presumption of the applicability of the
government contractor defense. In
determining whether to issue such
Certification, the Under Secretary or his
designee shall conduct a comprehensive
review of the design of such Technology
and determine whether it will perform
as intended, conforms to the Seller’s
specifications, and is safe for use as
intended. The Seller shall provide safety
and hazard analyses and other relevant
data and information regarding such
Qualified Anti-Terrorism Technology to
the Department in connection with an
application. The Under Secretary or his
designee may require that the Seller
submit any information that the Under
Secretary or his designee considers
relevant to the application for approval.
The Under Secretary or his designee
may consult with, and rely upon the
expertise of, any other governmental or
non-governmental person, firm, or
entity, and may consider test results
produced by an independent laboratory
or other person, firm, or other entity
engaged by the Seller.

(b) Extent of Liability. Should a
product liability or other lawsuit be
filed for claims arising out of, relating
to, or resulting from an Act of Terrorism
when Qualified Anti-Terrorism
Technologies Certified by the Under
Secretary as provided in §§ 25.8 and
25.9 of this part have been deployed in
defense against or response or recovery
from such act and such claims result or
may result in loss to the Seller, there
shall be a rebuttable presumption that
the government contractor defense
applies in such lawsuit. This
presumption shall only be overcome by
clear and convincing evidence showing
that the Seller acted fraudulently or
with willful misconduct in submitting
information to the Department during
the course of the consideration of such
Technology under this section and
§ 25.9 of this part. A claimant’s burden
to show fraud or willful misconduct
in connection with a Seller’s SAFETY Act
application cannot be satisfied unless
the claimant establishes there was a
knowing and deliberate intent to
deceive the Department. This
presumption of the government
defender shall apply
regardless of whether the claim against
the Seller arises from a sale of the
product to Federal Government or non-
Federal Government customers. Such
presumption shall apply in perpetuity
to all deployments of a Qualified Anti-
Terrorism Technology (for which a
Certification has been issued by the
Under Secretary as provided in this
section and § 25.9 of this part) in
defense against, response to, or recovery
from any Act of Terrorism that occurs
on or after the effective date of the
Certification applicable to such
Technology, provided that the sale of
such Technology was consummated by
the Seller on or after the earliest date of
sale of such Technology specified in
such Certification (which shall be
determined by the Under Secretary in
his discretion, and may be prior to, but
shall not be later than, such effective
date) and prior to the expiration or
termination of such Certification.

(c) Establishing Applicability of the
Government Contractor Defense. The
Under Secretary will be exclusively
responsible for the review and approval
of anti-terrorism Technology for
purposes of establishing the government
contractor defense in any product
liability lawsuit for claims arising out
of, relating to, or resulting from an Act
of Terrorism when Qualified Anti-
Terrorism Technologies approved by the
Under Secretary, as provided in this
final rule, have been deployed in
defense against or response or recovery
from such act and such claims result or
may result in loss to the Seller. The
Certification of a Technology as an
Approved Product for Homeland
Security shall be the only evidence
necessary to establish that the Seller of
the Qualified Anti-Terrorism
Technology that has been issue a
Certification is entitled to a
presumption of dismissal from a cause
of action brought against a Seller arising
out of, relating to, or resulting from an
Act of Terrorism when the Qualified
Anti-Terrorism Technology was
deployed in defense against or response
to or recovery from such Act of
Terrorism. This presumption of
dismissal is based upon the statutory
government contractor defense
conferred by the SAFETY Act.

§ 25.9 Procedures for Certification of
Approved Products for Homeland Security.

(a) Application Procedure. An
applicant seeking a Certification of anti-
terrorism Technology as an Approved
Product for Homeland Security under
§ 25.8 shall submit information
supporting such request to the Under
Secretary. The Under Secretary shall
make application forms available at
http://www.safetyact.gov, and copies
may also be obtained by mail by sending
a request to: Directorate of Science and
Technology, SAFETY Act/room 4320,
Department of Homeland Security,
Washington, DC 20528. An application
for a Certification may not be filed
unless the applicant has also filed an
application for a Designation for the
same Technology in accordance with
§ 25.6(a). Such applications may be filed
simultaneously and may be reviewed
simultaneously by the Department.
(b) Initial Notification. Within 30 days after receipt of an application for a Certification, the Under Secretary or his designee shall notify the applicant in writing that:

(1) The application is complete and will be reviewed, or

(2) That the application is incomplete, in which case the missing or incomplete parts will be specified.

(c) Review Process. The Under Secretary or his designee will review each complete application for a Certification and any included supporting materials. In performing this function, the Under Secretary or his designee may, but is not required to:

(1) Request additional information from the Seller;

(2) Meet with representatives of the Seller;

(3) Consult with, and rely upon the expertise of, any other Federal or non-Federal entity; and

(4) Perform or seek studies or analyses of the Technology.

(d) Action by the Under Secretary.

(1) Within 90 days after receipt of a complete application for a Certification, the Under Secretary shall take one of the following actions:

(i) Approve the application and issue an appropriate Certification to the Seller;

(ii) Notify the Seller in writing that the Technology is potentially eligible for a Certification, but that additional specified information is needed before a decision may be reached; or

(iii) Deny the application, and notify the Seller in writing of such decision.

(2) The Under Secretary may extend the time period one time for 45 days upon notice to the Seller, and the Under Secretary is not required to provide a reason or cause for such extension. The Under Secretary’s decision shall be final and not subject to review, except at the discretion of the Under Secretary.

(e) Designation is a Pre-Condition.

The Under Secretary may approve an application for a Certification only if the Under Secretary has also approved an application for a Designation for the same Technology in accordance with § 25.4.

(f) Content and Term of Certification; Renewal. (1) A Certification shall:

(i) Describe the Qualified Anti-Terrorism Technology (in such detail as the Under Secretary deems to be appropriate);

(ii) Identify the Seller(s) of the Qualified Anti-Terrorism Technology;

(iii) Specify the earliest date of sale of the Qualified Anti-Terrorism Technology that the Certification shall apply (which shall be determined by the Under Secretary in his discretion, and may be prior to, but shall not be later than, the effective date of the Certification); and

(iv) To the extent practicable, include such standards, specifications, requirements, performance criteria, limitations, or other information as the Department in its sole and unreviewable discretion may deem appropriate.

(2) A Certification shall be valid and effective for the same period of time for which the related Designation is issued, and shall terminate upon the termination of such related Designation. The Seller may apply for renewal of the Certification in connection with an application for renewal of the related Designation. An application for renewal must be made using the “Application for Certification of an Approved Product for Homeland Security” form issued by the Under Secretary.

(g) Application of Certification to Licensees. A Certification shall apply to any other person, firm, or other entity to which the applicable Seller licenses (exclusively or nonexclusively) the right to manufacture, use, or sell the Technology, in the same manner and to the same extent that such Certification applies to the Seller, effective as of the date of commencement of the license, provided that the Seller notifies the Under Secretary of such license by submitting, within 30 days after such date of commencement, a “Notice of License of Approved Anti-terrorism Technology” form issued by the Under Secretary. The Under Secretary shall make this form available at http://www.safetyact.gov and by mail upon request sent to: Directorate of Science and Technology, SAFETY Act/room 4320, Department of Homeland Security, Washington, DC 20528. Such notification shall not be required for any licensee listed as a Seller on the applicable Certification.

(h) Transfer of Certification. In the event of any permitted transfer and assignment of a Designation, any related Certification for the same anti-terrorism Technology shall automatically be deemed to be transferred and assigned to the same transferee to which such Designation is transferred and assigned. The transferred Certification will continue to apply to the transferee with respect to all transactions and occurrences that occurred through the time at which such transfer and assignment of the Certification became effective.

(i) Issuance of Certificate; Approved Product List. For anti-terrorism Technology reviewed and approved by the Under Secretary under which a Certification is issued, the Under Secretary shall issue a certificate of conformance to the Seller and place the anti-terrorism Technology on an Approved Product List for Homeland Security, which shall be published by the Department.

(j) Block Certifications. (1) From time to time, the Under Secretary, in response to an application submitted pursuant to § 25.9(a) or at his own initiative, may issue a Certification that is applicable to any person, firm or other entity that is a qualified Seller of the Approved Product for Homeland Security described in such Certification (a “Block Certification”). All Block Certifications shall be published by the Department within ten days after the issuance thereof at http://www.safetyact.gov, and copies may also be obtained by mail by sending a request to: Directorate of Science and Technology, SAFETY Act/room 4320, Department of Homeland Security, Washington, DC 20528. Any person, firm, or other entity that desires to qualify as a Seller of an Approved Product for Homeland Security under a Block Certification may complete only such portions of the application referenced in § 25.9(a) as are specified in such Block Certification and shall submit such application to the Department in accordance with § 9(a). Applicants seeking to be qualified Sellers of an Approved Product for Homeland Security pursuant to a Block Certification will receive expedited review of their applications and shall not be required to provide information with respect to the technical merits of the Approved Product for Homeland Security that has received Block Certification. Within 60 days (or such other period of time as may be specified in the applicable Block Certification) after the receipt by the Department of a complete application, the Under Secretary shall take one of the following actions:

(i) Approve the application and notify the applicant in writing of such approval; or

(ii) Deny the application, and notify the applicant in writing of such decision, including the reasons for such denial.

(2) If the application is approved, commencing on the date of such approval, the applicant shall be deemed to be a Seller under the applicable Block Certification for all purposes under the SAFETY Act, this part, and such Block Certification. A Block Certification shall be valid and effective for the same period of time for which the related Block Designation is issued. A Block Certification may be removed by the Under Secretary at his own initiative or in response to an application for...
§ 25.10 Confidentiality and Protection of Intellectual Property.

(a) General. The Secretary, in consultation with the Office of Management and Budget and appropriate Federal law enforcement and intelligence officials, and in a manner consistent with existing protections for sensitive or classified information, shall establish confidentiality procedures for safeguarding, maintenance and use of information submitted to the Department under this part. Such protocols shall, among other things, ensure that the Department will utilize all appropriate exemptions from the Freedom of Information Act.

(b) Non-Disclosure. Except as otherwise required by applicable law or regulation or a final order of a court of competent jurisdiction, or as expressly authorized in writing by the Under Secretary, no person, firm, or other entity may:

(1) Disclose SAFETY Act Confidential Information (as defined above) to any person, firm, or other entity, or

(2) Use any SAFETY Act Confidential Information for his, her, or its own benefit or for the benefit of any other person, firm, or other entity, unless the applicant has consented to the release of such SAFETY Act Confidential Information.

(c) Legends. Any person, firm, or other entity that submits data or information to the Department under this Part may place a legend on such data or information indicating that the submission constitutes SAFETY Act Confidential Information. The absence of such a legend shall not prevent any data or information submitted to the Department under this Part from constituting or being considered by the Department to constitute SAFETY Act Confidential Information.

DEPARTMENT OF AGRICULTURE

Animal and Plant Health Inspection Service

7 CFR Part 301

[Docket No. APHIS–2006–0033]

RIN 0579–AC05

Citrus Canker; Compensation for Certified Citrus Nursery Stock

AGENCY: Animal and Plant Health Inspection Service, USDA.

ACTION: Interim rule and request for comments.

SUMMARY: We are amending the citrus canker regulations to establish provisions under which eligible commercial citrus nurseries may, subject to the availability of appropriated funds, receive payments for certified citrus nursery stock destroyed to eradicate or control citrus canker. The payment of these funds will reduce the economic effects on commercial citrus nurseries that have had certified citrus nursery stock destroyed to control citrus canker.

DATES: This interim rule is effective June 8, 2006. We will consider all comments that we receive on or before August 7, 2006.

ADDRESSES: You may submit comments by either of the following methods:

Postal Mail/Commercial Delivery: 5223 Postal Mail and Commercial Delivery to

http://www.regulations.gov

ADDRESSES: You may submit comments by either of the following methods:

Federal e-rulemaking Portal: Go to http://www.regulations.gov and, in the lower “Search Regulations and Federal Actions” box, select “Animal and Plant Health Inspection Service” from the agency drop-down menu, then click on “Submit.” In the Docket ID column, select APHIS–2006–0033 to submit or view public comments and to view supporting and related materials available electronically. Information on using Regulations.gov, including instructions for accessing documents, submitting comments, and viewing the docket after the close of the comment period, is available through the site’s “User Tips” link.

Postal Mail/Commercial Delivery: Please send four copies of your comment (an original and three copies) to Docket No. APHIS–2006–0033, Regulatory Analysis and Development, PPD, APHIS, Station 3A–03.8, 4700 River Road Unit 118, Riverdale, MD 20737–1238. Please state that your comment refers to Docket No. APHIS–2006–0033.

Reading Room: You may read any comments that we receive on this docket in our reading room. The reading room is located in room 1141 of the USDA South Building, 14th Street and Independence Avenue, SW., Washington, DC. Normal reading room hours are 8 a.m. to 4:30 p.m., Monday through Friday, except holidays. To be sure someone is there to help you, please call (202) 690–2817 before coming.

Other Information: Additional information about APHIS and its programs is available on the Internet at http://www.aphis.usda.gov.

FOR FURTHER INFORMATION CONTACT: Mr. Stephen R. Poe, Operations Officer, Program Support Staff, PPQ, APHIS, 4700 River Road Unit 36, Riverdale, MD 20737–1231; (301) 734–8899.

SUPPLEMENTARY INFORMATION:

Background

Citrus canker is a plant disease that affects plants and plant parts, including fresh fruit, of citrus and citrus relatives (Family Rutaceae). Citrus canker can cause defoliation and other serious damage to the leaves and twigs of susceptible plants. It can also cause lesions on the fruit of infected plants, which render the fruit unmarketable, and cause infected fruit to drop from the trees before reaching maturity. The aggressive A (Asiatic) strain of citrus canker can infect susceptible plants rapidly and lead to extensive economic losses in commercial citrus-producing areas.

The regulations to prevent the interstate spread of citrus canker are contained in §§ 301.75–1 through 301.75–14 of “Subpart-Citrus Canker” in Title 7 of the Code of Federal Regulations. These regulations restrict the interstate movement of regulated articles from and through areas quarantined because of citrus canker and provide conditions under which regulated fruit may be moved into, through, and from quarantined areas for packing. These regulations were promulgated pursuant to the Plant Protection Act (7 U.S.C. 7701–7772). The regulations in §§ 301.75–15 and 301.75–16 (referred to below as the regulations) of “Subpart-Citrus Canker” provide for compensation to owners of commercial citrus groves for losses due to citrus canker eradication activities under certain conditions. Section 301.75–15 addresses compensation for commercial citrus trees and § 301.75–16 focuses on compensation for the recovery of lost production income. These regulations were promulgated to implement the appropriations statutes enacted in 2000.

In February 2003, Congress appropriated funds to compensate commercial citrus and lime growers in the State of Florida for lost...
Subtitle G—Support Anti-terrorism by Fostering Effective Technologies Act of 2002

SEC. 861. SHORT TITLE.
This subtitle may be cited as the “Support Anti-terrorism by Fostering Effective Technologies Act of 2002” or the “SAFETY Act”.

SEC. 862. ADMINISTRATION.
(a) IN GENERAL.—The Secretary shall be responsible for the administration of this subtitle.

(b) DESIGNATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGIES.—The Secretary may designate anti-terrorism technologies that qualify for protection under the system of risk management set forth in this subtitle in accordance with criteria that shall include, but not be limited to, the following:

(1) Prior United States Government use or demonstrated substantial utility and effectiveness.

(2) Availability of the technology for immediate deployment in public and private settings.

(3) Existence of extraordinarily large or extraordinarily unquantifiable potential third party liability risk exposure to the Seller or other provider of such anti-terrorism technology.

(4) Substantial likelihood that such anti-terrorism technology will not be deployed unless protections under the system of risk management provided under this subtitle are extended.

(5) Magnitude of risk exposure to the public if such antiterrorism technology is not deployed.

(6) Evaluation of all scientific studies that can be feasibly conducted in order to assess the capability of the technology to substantially reduce risks of harm.

(7) Anti-terrorism technology that would be effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat or respond to such acts.

(c) REGULATIONS.—The Secretary may issue such regulations, after notice and comment in accordance with section 553 of title 5, United States Code, as may be necessary to carry out this subtitle.

SEC. 863. LITIGATION MANAGEMENT.
(a) FEDERAL CAUSE OF ACTION.—
(1) IN GENERAL.—There shall exist a Federal cause of action for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. The substantive law for decision in any such action shall be derived from the law, including choice of law principles, of the State in which such acts of terrorism occurred, unless such law is inconsistent with or preempted by Federal law. Such Federal cause of action shall be brought only for claims for injuries that are proximately caused by sellers that provide qualified anti-terrorism technology to Federal and non-Federal government customers.

(2) JURISDICTION.—Such appropriate district court of the United States shall have original and exclusive jurisdiction over all actions for any claim for loss of property, personal injury, or death arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller.
(b) **SPECIAL RULES.**—In an action brought under this section for damages the following provisions apply:

(1) **PUNITIVE DAMAGES.**—No punitive damages intended to punish or deter, exemplary damages, or other damages not intended to compensate a plaintiff for actual losses may be awarded, nor shall any party be liable for interest prior to the judgment.

(2) **NONECONOMIC DAMAGES.**—

(A) **IN GENERAL.**—Noneconomic damages may be awarded against a defendant only in an amount directly proportional to the percentage of responsibility of such defendant for the harm to the plaintiff, and no plaintiff may recover noneconomic damages unless the plaintiff suffered physical harm.

(B) **DEFINITION.**—For purposes of subparagraph (A), the term “noneconomic damages” means damages for losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companionship, loss of consortium, hedonic damages, injury to reputation, and any other nonpecuniary losses.

(c) **COLLATERAL SOURCES.**—Any recovery by a plaintiff in an action under this section shall be reduced by the amount of collateral source compensation, if any, that the plaintiff has received or is entitled to receive as a result of such acts of terrorism that result or may result in loss to the Seller.

(d) **GOVERNMENT CONTRACTOR DEFENSE.**—

(1) **IN GENERAL.**—Should a product liability or other lawsuit be filed for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies approved by the Secretary, as provided in paragraphs (2) and (3) of this subsection, have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller, there shall be a rebuttable presumption that the government contractor defense applies in such lawsuit. This presumption shall only be overcome by evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the course of the Secretary’s consideration of such technology under this subsection. This presumption of the government contractor defense shall apply regardless of whether the claim against the Seller arises from a sale of the product to Federal Government or non-Federal Government customers.

(2) **EXCLUSIVE RESPONSIBILITY.**—The Secretary will be exclusively responsible for the review and approval of antiterrorism technology for purposes of establishing a government contractor defense in any product liability lawsuit for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies approved by the Secretary, as provided in this paragraph and paragraph (3), have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. Upon the Seller’s submission to the Secretary for approval of anti-terrorism technology, the Secretary will conduct a comprehensive review of the design of such technology and determine whether it will perform as intended, conforms to the Seller’s specifications, and is safe for use as intended. The Seller will conduct safety and hazard analyses on such technology and will supply the Secretary with all such information.

(3) **CERTIFICATE.**—For anti-terrorism technology reviewed and approved by the Secretary, the Secretary will issue a certificate of conformance to the Seller and place the antiterrorism technology on an Approved Product List for Homeland Security.

(e) **EXCLUSION.**—Nothing in this section shall in any way limit the ability of any person to seek any form of recovery from any person, government, or other entity that—

(1) attempts to commit, knowingly participates in, aids and abets, or commits any act of terrorism, or any criminal act related to or resulting from such act of terrorism; or (2) participates in a conspiracy to commit any such act of terrorism or any such criminal act.
SEC. 864. RISK MANAGEMENT.

(a) IN GENERAL.—
(1) LIABILITY INSURANCE REQUIRED.—Any person or entity that sells or otherwise provides a qualified anti-terrorism technology to Federal and non-Federal Government customers ("Seller") shall obtain liability insurance of such types and in such amounts as shall be required in accordance with this section and certified by the Secretary to satisfy otherwise compensable third-party claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act.

(2) MAXIMUM AMOUNT.—For the total claims related to 1 such act of terrorism, the Seller is not required to obtain liability insurance of more than the maximum amount of liability insurance reasonably available from private sources on the world market at prices and terms that will not unreasonably distort the sales price of Seller’s anti-terrorism technologies.

(3) SCOPE OF COVERAGE.—Liability insurance obtained pursuant to this subsection shall, in addition to the Seller, protect the following, to the extent of their potential liability for involvement in the manufacture, qualification, sale, use, or operation of qualified anti-terrorism technologies deployed in defense against or response or recovery from an act of terrorism:

(A) Contractors, subcontractors, suppliers, vendors and customers of the Seller.

(B) Contractors, subcontractors, suppliers, and vendors of the customer.

(4) THIRD PARTY CLAIMS.—Such liability insurance under this section shall provide coverage against third party claims arising out of, relating to, or resulting from the sale or use of anti-terrorism technologies.

(b) RECIPROCAL WAIVER OF CLAIMS.—The Seller shall enter into a reciprocal waiver of claims with its contractors, subcontractors, suppliers, vendors and customers, and contractors and subcontractors of the customers, involving in the manufacture, sale, use or operation of qualified anti-terrorism technologies, under which each party to the waiver agrees to be responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act.

(c) EXTENT OF LIABILITY.—Notwithstanding any other provision of law, liability for all claims against a Seller arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller, whether for compensatory or punitive damages or for contribution or indemnity, shall not be in an amount greater than the limits of liability insurance coverage required to be maintained by the Seller under this section.

SEC. 865. DEFINITIONS.

For purposes of this subtitle, the following definitions apply:

(1) QUALIFIED ANTI-TERRORISM TECHNOLOGY.—For purposes of this subtitle, the term "qualified anti-terrorism technology" means any product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, that is designated as such by the Secretary.

(2) ACT OF TERRORISM.—(A) The term "act of terrorism" means any act that the Secretary determines meets the requirements under subparagraph (B), as such requirements are further defined and specified by the Secretary.

(B) REQUIREMENTS.—An act meets the requirements of this subparagraph if the act—

(i) is unlawful;
(ii) causes harm to a person, property, or entity, in the United States, or in the case of a domestic United States air carrier or a United States-flag vessel (or a vessel based principally in the United States on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), in or outside the United States; and (iii) uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.

(3) INSURANCE CARRIER.—The term ‘‘insurance carrier’’ means any corporation, association, society, order, firm, company, mutual, partnership, individual aggregation of individuals, or any other legal entity that provides commercial property and casualty insurance. Such term includes any affiliates of a commercial insurance carrier.

(4) LIABILITY INSURANCE.—
(A) IN GENERAL.—The term ‘‘liability insurance’’ means insurance for legal liabilities incurred by the insured resulting from—

(i) loss of or damage to property of others;
(ii) ensuing loss of income or extra expense incurred because of loss of or damage to property of others;
(iii) bodily injury (including) to persons other than the insured or its employees; or
(iv) loss resulting from debt or default of another.

(5) LOSS.—The term ‘‘loss’’ means death, bodily injury, or loss of or damage to property, including business interruption loss.

(6) NON-FEDERAL GOVERNMENT CUSTOMERS.—The term ‘‘non-Federal Government customers’’ means any customer of a Seller that is not an agency or instrumentality of the United States Government with authority under Public Law 85–804 to provide for indemnification under certain circumstances for third-party claims against its contractors, including but not limited to State and local authorities and commercial entities.
Chemicals are vital to our economy. They are used to develop medicines that maintain our health, provide refrigeration for our food supply, manufacture fuel for our vehicles and build the microchip that runs our smartphones. In the hands of a terrorist, however, chemicals could potentially be used to cause a significant number of deaths and injuries. The U.S. Department of Homeland Security, through the Infrastructure Security Compliance Division (ISCD), administers the Chemical Facility Anti-Terrorism Standards (CFATS) program by working with facilities to ensure they have security measures in place to reduce the risk of certain hazardous chemicals being exploited in an attack.

**What is CFATS?**

CFATS is a regulatory program (6 CFR Part 27) established in 2007 that addresses chemical security by identifying and regulating high-risk chemical facilities that possess chemicals of interest (COI) at specific concentrations and quantities. In 2014, Congress reauthorized and amended the program through the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (6 U.S.C. § 621, et seq).

Appendix A of the CFATS regulation lists more than 300 COI and their respective screening threshold quantities (STQ). Any facility that meets or exceeds the STQ for any COI is required to submit an online survey, known as the Top-Screen, within 60 days of coming in possession of the COI.

**What is Risk-Based Tiering?**

The CFATS regulation follows a risk-based approach that allows ISCD to focus its resources on high-risk chemical facilities. To identify a facility’s specific level of risk, DHS analyzes information submitted through the Top-Screen to determine which facilities are high-risk and assign those facilities to one of four tiers with Tier 1 representing the highest-risk.

**Enhanced Tiering Methodology**

In 2013, DHS undertook a thorough review of the CFATS risk-tiering methodology. This included a peer review of the prior methodology conducted by a panel of experts drawn from across industry, academia, and government; a review of the proposed new methodology by external experts from industry, government, and the Homeland Security Studies and Analysis Institute; and an independent verification by Sandia National Laboratories.

In 2016, DHS rolled out the enhanced risk-tiering methodology that more accurately identifies and appropriately tiers high-risk chemical facilities. The improved methodology considers three main elements in a facility’s high-risk determination:

- Vulnerability
- Consequence
- Threat

While much of the methodology is sensitive and/or classified, the following tables provide information to help facilities better understand the types of items that may impact their high-risk status and, as applicable, their risk tiers.
Vulnerability
The vulnerability variable considers inherent characteristics of the facility and/or assets that reduce vulnerability to a terrorist attack—for example, a COI storage container located in an underground earth formation.

<table>
<thead>
<tr>
<th>Factors Considered to Reduce Vulnerability</th>
<th>Applicable Security Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Higher design pressure of a storage container</td>
<td>• Release</td>
</tr>
<tr>
<td>Below-grade storage</td>
<td>• Release</td>
</tr>
<tr>
<td>Larger, less portable COI containers</td>
<td>• Theft</td>
</tr>
</tbody>
</table>
| COI is not shipped from the facility       | • Diversion  
                     | • Sabotage |

Consequence
The consequence variable incorporates improved tools that allow DHS to more accurately calculate, through physics-based dispersion and blast modeling, the onsite and offsite impacts of COI exploitation and misuse.

<table>
<thead>
<tr>
<th>Factors Considered for Consequence</th>
<th>Applicable Security Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topography surrounding facility (urban or rural terrain)</td>
<td>• Release</td>
</tr>
<tr>
<td>Potentially exposed population surrounding facility</td>
<td>• Release</td>
</tr>
</tbody>
</table>
| COI toxicity                        | • Release—toxics  
                     | • Theft/Diversion—Weapons of Mass Effect/Chemical Weapons  
                     | • Sabotage |
| COI flammability                    | • Release |
| COI explosive energy                | • Release—Explosives (EXP)  
                     | • Theft/Diversion—Explosives/Improvised Explosive Device |
| COI quantity and concentration      | • Release  
                     | • Theft/Diversion  
                     | • Sabotage |
| COI storage: container location and pressure rating | • Release |
| COI storage: types of packaging     | • Theft/Diversion |
| COI precursor characteristics: toxicity/explosive energy | • Theft/Diversion—Chemical Weapons Precursors/IEDPs |
| Mode of shipping                    | • Sabotage |

Threat
The threat variable includes factors informed by the intelligence community that may affect the level of threat of terrorist attack or exploitation for a facility.

<table>
<thead>
<tr>
<th>Factors Considered for Threat</th>
<th>Applicable Security Issue</th>
</tr>
</thead>
</table>
| Specific COI                  | • Release  
                     | • Theft/Diversion |
| Mode of shipment              | • Theft/Diversion  
                     | • Sabotage |

Tools and Resources
- For the latest information about the risk-tiering methodology, visit www.dhs.gov/cfats-tiering-methodology.
- The CSAT Help Desk provides timely support to chemical facility owners and operators. Call 1-866-323-2957 or email csat@hq.dhs.gov.

Contact Information
To discuss your specific facility’s risk, you may speak with a Compliance Case Manager or Chemical Security Inspector. For any questions, comments or concerns, please contact CFATS@hq.dhs.gov or visit www.dhs.gov/chemicalsecurity.
Chemicals are vital to our Nation’s economy, and protecting chemicals from being used or exploited in a terrorist attack is a shared commitment between the Federal government, the private sector, and members of the community, including law enforcement, hazmat, and emergency responders.

The Chemical Facility Anti-Terrorism Standards (CFATS) program identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with their chemicals. Under CFATS, facilities that DHS has identified as high-risk are required to develop and implement security plans that meet the risk-based performance standards (RBPS). DHS and high-risk chemical facilities work in unison with State and local emergency responders and law enforcement to ensure that appropriate emergency response measures are in place in the event of an incident.

The CFATS Program at a Glance

DHS identified 322 chemicals of interest (COI) that facilities must report if possessed in certain quantities. These chemicals could be used by a terrorist to cause harm if deliberately released or stolen and misused as weapons. More than 60,000 facilities—ranging from oil refineries and microchip manufacturers, to fisheries and universities—have reported possessing chemicals to DHS. The Department uses the information facilities report to identify which facilities are high-risk and, therefore, covered by the CFATS program. More than 150 Chemical Security Inspectors are located in communities nationwide. These inspectors assist high-risk facilities identify security measures that are appropriate to their chemicals and conduct inspections to ensure agreed-upon security measures remain in place.

The Vital Role of the Emergency Responder

Security plans for CFATS-covered facilities must address not only cyber and physical security measures, but also training, standard operating procedures, and response capabilities. Including first responders when developing an emergency plan and conducting exercises establishes relationships, improves the responders’ understanding of the facility’s layout, and enables both the facility and local law enforcement to take quick and decisive action in the case of an event.

How can Emergency Responders Assist DHS?

- **Meet your Region’s Chemical Security Inspectors.** Inspectors can assist emergency responders and law enforcement with identifying CFATS-covered facilities, identifying the chemicals those facilities possess, and understanding the possible dangers associated with those chemicals. For information on contacting an inspector, contact 1-866-323-2957 or CSAT@hq.dhs.gov.

- **Participate in Facility Drills and Exercises.** Emergency responders and law enforcement are often invited to participate in drills and exercises in their areas of responsibility. Take advantage of these opportunities; they can assist in understanding the layout and potential hazards at the facility. Additionally, these drills help alert participants to resources that may be needed in an event of a chemical incident.

- **Seek Out Training Opportunities.** Find out if there are local training opportunities available. For instance, the Emergency Management Institute offers virtual tabletop exercises on a monthly basis. A complete listing of Federal Emergency Management Agency’s (FEMA) exercise scenarios can be found at www.training.fema.gov/Programs/emiVTTX.aspx.
• **Report a Security Concern or CFATS Violation.** There are several ways to report a security concern: call the CFATS Tip Line at 1-877-FYI-4-DHS (1-877-394-4347) or send an email to CFATSTips@hq.dhs.gov. For additional information, please visit www.dhs.gov/report-cfats-violation.

**Chemical-Terrorism Vulnerable Information (CVI) and Emergency Responders**

Information about the security operations of CFATS-covered facilities is categorized as “Chemical-terrorism Vulnerability Information” (CVI) and requires certain protections from public disclosure or misuse. DHS provides each CVI Authorized User with a unique identification number. Except in exigent or emergency circumstances, CVI may only be disclosed to CVI Authorized Users with a need-to-know.

DHS encourages facilities to include law enforcement and emergency responders in the development and exercising of an emergency plan. While the majority of information needed by emergency responders is not CVI, certain situations may arise where CFATS-covered facilities would need to share some CVI with emergency responders. In these instances, the emergency responder should complete CVI training. DHS will then make a determination on their need-to-know. More information on CVI training can be accessed at www.dhs.gov/cvi-authorized-user-training.

**Tools and Resources for Emergency Responders**

- **Chemical Security Inspectors and other DHS subject matter experts** are available to provide guidance to facilities through outreach meetings, calls, and other engagements. To request a visit or meeting with a Chemical Security Inspector or to request a CFATS presentation, please contact cfats@hq.dhs.gov.

- The **Infrastructure Protection (IP) Gateway** serves as the single interface through which Federal, State, local, tribal, territorial, and private sector partners can identify, analyze, and manage risk to protect the nation. Visit www.dhs.gov/ipgateway or contact IPgateway@hq.dhs.gov for more information.

- The **CFATS Knowledge Center** is an online repository of Frequently Asked Questions, articles, and documents relating to CFATS that can be found by visiting csat-help.dhs.gov.

- The **CSAT Help Desk** provides timely support to chemical facility owners and operators and can be reached at 1-866-323-2957 or csat@hq.dhs.gov.

- **Emergency Management and Response—Information Sharing and Analysis Center** promotes critical infrastructure protection (CIP) by sharing CIP and emerging threats with Emergency Services Sector (ESS) departments and agencies nationwide. It provides access to ESS hazard information as well as current situation reports, public health bulletins, terrorism updates, and critical “For Official Use Only” information. For more information, visit www.usfa.fema.gov/emr-isac.

- The **Emergency Service Sector-Specific Agency** and the **Emergency Services Sector Coordinating Council** represents a collaborative effort among the private sector; State, local, tribal, and territorial governments; nongovernmental organizations; and Federal departments working toward achieving shared goals and to address the unique operating conditions and risk landscape of the Emergency Services Sector. For more information, visit www.dhs.gov/emergency-services-sector.

---

*June 2017*
Chemicals are vital to our economy. They are used to develop medicines that maintain our health, provide refrigeration for our food supply, manufacture fuel for our vehicles and build the microchip that runs our smartphones. But in the hands of a terrorist, chemicals could potentially be used to cause a significant number of deaths and injuries. The U.S. Department of Homeland Security, through the Infrastructure Security Compliance Division (ISCD), administers the CFATS program by working with facilities to ensure they have security measures in place to reduce the risks associated with certain hazardous chemicals, and prevent them from being exploited in an attack.

**What is CFATS?**

CFATS is a regulatory program (6 CFR Part 27) established in 2007 that addresses chemical security by identifying and regulating high-risk facilities that possess certain chemicals of interest (COI) at specific concentrations and quantities. In 2014, Congress reauthorized and amended the program through the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (6 U.S.C. § 621, et seq).

The CFATS regulation applies to facilities across many industries, including:

- Chemical manufacturing, storage, and distribution
- Energy and utilities
- Agriculture and food
- Explosives
- Mining
- Electronics
- Plastics
- Universities and laboratories
- Paint and coatings
- Healthcare and pharmaceuticals

**Appendix A and Chemicals of Interest**

Appendix A of the CFATS regulation (6 CFR Part 27) lists more than 300 COI and their respective screening threshold quantities (STQ). These COI are categorized into three main security issues.

- **Release**: Toxic, flammable, or explosive chemicals or materials that can be released at a facility.
- **Theft or Diversion**: Chemicals or materials that, if stolen or diverted, can be converted into weapons using simple chemistry, equipment, or techniques.
- **Sabotage**: Chemicals or materials that can be mixed with readily available materials.

Any facility that meets or exceeds the STQ for any COI listed in Appendix A is required to report possession of those chemicals to DHS via an online questionnaire called a Top-Screen.
The CFATS Process

1. If not statutorily excluded from CFATS\(^1\), read Appendix A (www.dhs.gov/publication/appendix-final-rule) to determine if your facility manufactures, stores, or distributes any of the COI at or above the STQ. If your facility possesses COI at or above STQ, complete a Top-Screen (www.dhs.gov/cفاتs-top-screen) about your chemical holdings via the Chemical Security Assessment Tool (CSAT).

2. ISCD reviews Top-Screens using a risk-based methodology. Facilities are notified if they are:
   - Determined to be a high-risk facility and ranked into Tiers 1, 2, 3, and 4, with Tier 1 being the highest risk.
   - Determined not to be a high-risk facility and not regulated under CFATS.

3. If your facility is tiered, your facility must submit a Security Vulnerability Assessment (SVA) and a Site Security Plan (SSP)—or an Alternative Security Program (ASP)—that meets the risk-based performance standards (RBPS) (www.dhs.gov/cfats-risk-based-performance-standards) specified in the CFATS regulation.
   - The 18 RBPS address security issues such as perimeter security, access control, personnel security, cyber security, etc.
   - Your facility’s security plan is tailored to its tier level, risk, and circumstances.

4. ISCD Inspectors perform an authorization inspection at your facility prior to approving the security plan.
   - Once the plan is approved, inspectors conduct regular compliance inspections to verify your facility implements the agreed-upon security measures.

CFATS Enforcement Actions

ISCD is committed to helping facility personnel understand and comply with CFATS by providing technical assistance or onsite consultation. However, ISCD is authorized to pursue civil enforcement action against any facility found in violation of CFATS, which could result in the imposition of a civil fine and/or the issuance of an order to cease operations. Violations vary from a facility refusing to report its COI holdings, failing to develop and/or implement certain security measures, or knowingly providing false information. ISCD will specify the nature of violation(s) and steps that must be taken to correct the noncompliance before fines are assessed. The maximum civil penalty is $33,333 for each day a violation continues.

Tools and Resources

- Request a CFATS Presentation to learn about any part of the CFATS regulation from submitting a Top-Screen to editing a security plan: www.dhs.gov/request-cfats-presentation.
- Request a Compliance Assistance Visit to learn what to expect from a CFATS Authorization or Compliance Inspection: www.dhs.gov/cfats-request-compliance-assistance-visit.
- The Chemical Security Assessment Tool Help Desk provides timely support to chemical facility owners and operators. Call 1-866-323-2957 or email csat@hq.dhs.gov.
- The CFATS Knowledge Center is an online repository of Frequently Asked Questions, articles, and documents relating to CFATS. Visit the CFATS Knowledge Center at csat-help.dhs.gov/.

Contact Information

For any questions, comments, or concerns, please contact CFATS@hq.dhs.gov or visit www.dhs.gov/chemicalsecurity.

\(^1\) Section 2101 of the CFATS Act of 2014 defined excluded facility as: a facility regulated under the Maritime Transportation Security Act of 2002; a public water systems as defined in the Safe Drinking Water Act; a Treatment Works as defined in the Federal Water Pollution Control Act; a facility owned or operated by the Department of Defense or the Department of Energy; and a facility subject to regulation by the Nuclear Regulatory Commission.
CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (CFATS)
Why Chemical Facility Security?

- We face a persistent and evolving threat
- A successful attack on a chemical facility could potentially cause a significant number of deaths and injuries
- Certain chemical facilities possess materials that could be stolen or diverted and used for terrorist activities
Ensuring Chemical Facility Security

Statutory Authority

- December 2006 – Congress authorized DHS to regulate security at “high-risk” chemical facilities

- DHS developed the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27, to implement this authority

- December 2014 – Congress extended CFATS the program through the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 - 6 U.S. Code Chapter 1, Subchapter XVI: Chemical Facility Anti-Terrorism Standards (CFATS)

- January 2019 – CFATS received a 15-month extension to its current authorization
CFATS identifies and regulates high-risk chemical facilities to ensure they implement appropriate security measures to reduce the risk of a terrorist attack associated with more than 300 chemicals of interest (COI).

Facilities that store, manufacture, or distribute COI at or above screening threshold quantities (STQ) must report them to CISA in compliance with CFATS.

- CFATS follows a risk-based approach, allowing CISA to focus on high-risk chemical facilities in accordance with their specific level of risk.
CFATS Universe

Identifying high-risk chemical facilities

- “Appendix A” – a list of 300+ chemicals of interest (COI), which at specific threshold quantities and concentrations, require reporting to the Department

Chemical Facilities Come in All Shapes and Sizes
Am I Exempt?

Statutory Exemptions

- Facilities regulated by the Nuclear Regulatory Commission
- Facilities owned by the Departments of Defense or Energy
- Public water systems and water treatment works regulated under certain Federal water quality laws
- Facilities regulated under the Maritime Transportation Security Act

Agricultural Production Facilities

- In January 2008, DHS indefinitely extended the Top-Screen due date for agricultural production facilities
The CFATS Process

Facility may be tiered in or drop out

If the facility receives a tier...

Submit Top-Screen

Receive a Tier (1-4) or be deemed not high-risk

Provide a Security Vulnerability Assessment (SVA)/Complete Site Security Plan (SSP) or Alternative Security Program (ASP)

Receive Authorization and an Authorization Inspection

Receive Approval of the SSP/ASP

Implement Planned Measures and Undergo Regular Compliance Inspections

All facilities with COI

High-risk facilities

- DHS provides compliance assistance upon request at any stage of this process

- More than 150 Chemical Security Inspectors are available for support across the country
Risk-Based Performance Standards

1) Restrict Area Perimeter  
2) Secure Site Assets  
3) Screen and Control Access  
4) Deter, Detect, Delay  
5) Shipping, Receipt, and Storage  
6) Theft and Diversion  
7) Sabotage  
8) Cyber  
9) Response  
10) Monitoring  
11) Training  
12) Personnel Surety  
13) Elevated Threats  
14) Specific Threats, Vulnerabilities, or Risks  
15) Reporting Significant Security Incidents  
16) Significant Security Incidents and Suspicious Activities  
17) Officials and Organization  
18) Records

- Rather than prescribe specific facility security measures, DHS developed 18 Risk-Based Performance Standards (RBPS)

- Compliance with the RBPS will be tailored to fit each facility’s circumstances, including tier level, security issues, and physical and operating environments
Explosive Precursor Chemicals

- Adversaries use explosive precursor chemicals in attacks worldwide—chemicals that are the focus of voluntary and/or regulatory controls in the EU, Canada, and other nations.
- DHS sponsored a study by the National Academy of Sciences—to provide options for a path forward to enhance controls for these chemicals in the United States.
- CISA is holding stakeholder engagement meetings to hear the industry’s opinion and expertise to help the Agency develop a broad, common-sense framework.

Los Angeles, CA  May 23, 2019
Orlando, FL  May 28, 2019
Houston, TX  June 4, 2019
Indianapolis, IN  June 11, 2019
Chicago, IL  June 13, 2019
CFATS National Footprint

Number of Facilities, by Region

- 0-200
- 201-400
- 401-600
- 600+

Puerto Rico
- Hawaii
- Guam

Region 1
Region 2
Region 3
Region 4
Region 5
Region 6
Region 7
Region 8
Region 9
Region 10

Puerto Rico (Region 2)
Hawaii (Region 9)
Guam (Region 9)