

**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 [Insert date 30 days after date of publication in the FEDERAL REGISTER].

**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:

(1) Web Site: <http://dms.dot.gov>.

(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.

(5) Federal eRulemaking portal: <http://www.regulations.gov>.

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 Towards 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. Deference 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 noneconomic 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 obtain insurance, 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 the 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. Arme) (“[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)(2); *See also* § 863(a)(1). This exclusive “Federal cause of action shall be brought only for claims for injuries that are proximately caused by sellers that provide qualified anti-terrorism technology.” § 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). That subsection states: "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." *Id.* Any presumption of concurrent causes of action (between state and Federal law) is overcome by two basic points. First, Congress would not have created in this Act a Federal cause of action to complement State law causes of action. Not only is the substantive law for decision in the Federal action derived from State law (and thus would be surplusage), but in creating the Act Congress plainly intended to limit rather than increase the liability exposure of Sellers. Second, the granting of exclusive jurisdiction to the Federal district courts provides further evidence that Congress wanted an exclusive Federal cause of action. Indeed, a

Federal district court (in the absence of diversity) does not have jurisdiction over State law claims, and the statute makes no mention of diversity claims anywhere in the Act.

Further, it is clear that the Seller is the only appropriate defendant in this exclusive Federal cause of action. First and foremost, the Act unequivocally states that a “cause of action shall be brought only for claims for injuries that are proximately caused by sellers that provide qualified anti-terrorism technology.” § 863(a)(1). Second, if the Seller of the Qualified Anti-Terrorism Technology at issue were not the only defendant, would-be plaintiffs could, in an effort to circumvent the statute, bring claims (arising out of or relating to the performance or non-performance of the Seller’s Qualified Anti-Terrorism Technology) against arguably less culpable persons or entities, including but not limited to contractors, subcontractors, suppliers, vendors, and customers of the Seller of the technology. Because the claims in the cause of action would be predicated on the performance or non-performance of the Seller’s Qualified Anti-Terrorism Technology, those persons or entities, in turn, would file a third-party action against the Seller. In such situations, the claims against non-Sellers thus “may result in loss to the Seller” under §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. Arme) (November 13, 2002) (stating that in some situations the SAFETY Act protections will “complement other government risk-sharing measures that some contractors can use such as Public Law 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 potentially 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 belief 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 in 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 website 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 efficiencies 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 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, in retrospect, 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 tension between 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 text 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 of the Technology as modified will be conclusively established. If the Department ultimately does not approve of the proposed changes, it will so 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 instrumentalities, 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 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 discernable. 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 incentivize 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 contactors, 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 continue to 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 Pub. L. 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 as 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 deployment 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 the 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 and the government procurement process 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) enable the selected contractor to receive expedited review of a streamlined application for SAFETY Act coverage and (ii) in 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 applications. 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 the Department with a description of their anti-terrorism technology 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-Terrorism 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 1**

#### 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.” Pub.L.107-297, 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 for interpretative rule 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 [www.safetyact.gov](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 removed and replaced with the following:

## **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.**

**Authority:** Subtitle G, of Title VIII, Pub. L. 107-296, 116 Stat. 2238 (6 U.S.C. 441-444).

**§ 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.

Certification – The term “Certification” 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 may include, without limitation, preparing the SAFETY Act Application Kit, receiving and facilitating the evaluation of applications, managing the SAFETY Act website 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 or Act – The term “SAFETY Act” or “Act” means the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, sections 441-444 of title 6, United States Code.

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. In determining whether to issue the Designation under paragraph (a), the Under Secretary may exercise discretion and judgment in considering the following criteria and evaluating the Technology:

(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 sections 441-444 of title 6, United States Code, are extended.

(5) Magnitude of risk exposure to the public if such anti-terrorism 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.

(8) 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.

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

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 categories 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 § 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 confidentiality 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) 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 (1) describe the subject Technology (in such detail as the Under Secretary deems to be appropriate), (2) identify the Seller of the subject Technology, (3) 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), (4) be terminable by the Under Secretary at any time upon notice to the Seller, (5) be subject to

the limitations on the use or deployment of the QATT set forth in the DT&E Designation, and (6) 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.

**§ 125.5 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. 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:

- (1) The particular Technology at issue;
- (2) The amount of liability insurance the Seller maintained prior to application;
- (3) The amount of liability insurance maintained by the Seller for other Technologies or for the Seller's business as a whole;
- (4) The amount of liability insurance typically maintained by Sellers of comparable Technologies;
- (5) Information regarding the amount of liability insurance offered on the world market;
- (6) Data and history regarding mass casualty losses;
- (7) The intended use of the Technology; and
- (8) 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.

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 unreasonably distort the sales price of the Seller's anti-terrorism Technology

(c) Scope of Coverage. 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:

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

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

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 (e) 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 a 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), 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. 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:

- (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;
- (4) perform studies or analyses of the subject Technology or the insurance market for such Technology; and
- (5) seek information from insurers regarding the availability of insurance for such Technology.

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:

- (1) Public source studies;
- (2) Classified and otherwise confidential studies;
- (3) Studies, tests, or other performance records or data provided by or available to the producer of the specific Technology; and
- (4) Proprietary studies that are available to the Under Secretary.

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 clause (1) of paragraph (b) 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. 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.

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, SAFETY Act/room 4320, Department of Homeland Security, Washington, DC 20528.

(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 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 section 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: (i) receive expedited review of their application for Designation; (ii) 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 (iii) 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 satisfy 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 for 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 Vendor(s), in relation to the criteria set forth in § 25.4(b), shall ordinarily consist of a validation that 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. 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:

- (1) approve the application and notify the applicant in writing of such approval, which notification shall include the certification required by § 25.5(g); or
- (2) deny the application, and notify the applicant in writing of such decision, including the reasons for such denial.

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 the 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. 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.

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 the preceding clause (v), 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.

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:

(i) 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;

(ii) 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

(iii) 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 section 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 of Terrorism 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 entity. 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 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. 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 section 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. 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 to which 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. 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 and 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 transferor 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 and for 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. 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 shall 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 § 25.9(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.

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 renewed by the Under Secretary at his own initiative or in response to an application for renewal submitted by a qualified Seller under such Block Certification in accordance with § 25.9(g). Except as otherwise specifically provided in this paragraph, a Block Certification shall be deemed to be a Certification for all purposes under the SAFETY Act and this Part.

**§ 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.

Dated: \_\_\_\_\_,

Michael Chertoff,  
Secretary