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: Interim rule with request for comments.

SUMMARY: This interim 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 Sellers of ''qualified anti-terrorism technologies.'' This rule provides the application process by which a seller will apply for liability protections for anti-terrorism technologies. Its purpose is to facilitate and promote the development and deployment of anti-terrorism technologies that will save lives.

DATES: This interim rule is effective October 16, 2003. Comments and related material must reach the Docket Management Facility on or before December 15, 2003. Comments sent to the Office of Management and Budget (OMB) on collection of information must reach OMB on or before December 15, 2003.

ADDRESSES: Because the Department of Homeland Security does not yet have electronic docketing capability, for the purposes of this rule, we are using the Department of Transportation Docket Management System for the U.S. Coast Guard. You may submit comments identified by Coast Guard docket number USCG–2003–15425 to the Docket Management Facility at the Department of Transportation. To avoid duplication, please use only 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.*

You must also mail comments on collection of information to the Office of Information and Regulatory Affairs, Office of Management and Budget, 725 17th Street, NW., Washington, DC 20503, ATTN: Desk Officer, Department of Homeland Security.

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 interim rule, call Wendy Howe, Directorate of Science and Technology, Department of Homeland Security, telephone 202–772–9887. 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:

Public Participation and Request for Comments

We encourage you to participate in this rulemaking by submitting comments and related materials. All comments received will be posted, without change, to *http://dms.dot.gov* and will include any personal information you have provided.

Submitting comments: If you submit a comment, please include your name and address, identify the docket number for this rulemaking (USCG–2003–15425), indicate the specific section of this document to which each comment applies, and give the reason for each comment. You may submit your comments and material by electronic means, mail, fax, or delivery to the Docket Management Facility at the address under **ADDRESSES**; but please submit your comments and material by only one means. If you submit them by mail or delivery, submit them in an unbound format, no larger than 8½ by 11 inches, suitable for copying and electronic filing. If you submit them by mail and would like to know that they reached the Facility, please enclose a stamped, self-addressed postcard or envelope. We will consider all comments and material received during the comment period. We may change this rule in view of them.

Viewing comments and document: To view comments, as well as documents mentioned in this preamble as being available in the docket, go to *http://dms.dot.gov* at any time and conduct a simple search using the docket number. You may also visit the Docket Management Facility in 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.

Privacy Act: Anyone can search the electronic form of all comments received in the docket by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.).

Regulatory History

On July 11, 2003, we published a notice of proposed rulemaking entitled ''Regulations Implementing the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act)'' in the **Federal Register** (68 FR 41420). No public hearing was requested and none was held. As stated in the notice of proposed rulemaking, we intended to implement this interim rule as soon as possible. The Department of Homeland Security (Department) finds that the need to foster anti-terrorism technology by instituting liability protection measures, as soon as practicable, furnishes good cause for this interim rule to take effect immediately under both the Administrative Procedure Act, 5 U.S.C. 552(d)(3), and section 808 of the Congressional Review 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 its statement of findings and purpose in 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 * * *.'' TRIA § 101(b)(2).

The United States remains at risk to terrorist attacks. It is in the public's interest to have this interim rule effective immediately because its aim is to foster the development and deployment of anti-terrorism technologies. Additionally, this interim rule will clarify to the greatest extent possible the application of the liability protections created by the SAFETY Act, thus providing an instant incentive for prospective applicants to apply for its protections and for others to begin exploring new measures that will prevent or reduce acts of terrorism. The interim rule will also provide the Department with sufficient program flexibility to address the specific circumstances of each particular request for SAFETY Act coverage. The application process is interactive. Those persons availing themselves of the protections afforded in this interim rule will also be interacting with the Department in the application process. Furthermore, the Department will continue to consider comments on this interim rule. Since the use of the liability protections afforded in this interim rulemaking is voluntary, there are no mandatory costs or burdens associated with the immediate implementation of this rule.

By having these provisions in place, the Department may begin processing applications for the liability protections and thus provide qualified Sellers of anti-terrorism technologies valuable incentives to develop and sell such technologies, as well as incentives for others to deploy such technologies. The purpose of those technologies is to detect, deter, mitigate, or assist in the recovery from a catastrophic act of terrorism. Thus, the Department finds that it is not only impracticable to delay an effective date of implementation, but it is also in the public's interest to make the interim rule effective upon publication in the **Federal Register**.

As previously mentioned in the proposed rule, the Department does not intend to resolve every conceivable programmatic issue through this interim rule. Instead, this interim rule sets out a basic set of regulations that implements the SAFETY Act program. The Department will continue to consider public comments and determine whether possible supplemental regulations are needed as we gain experience with implementing the Act.

Discussion of Comments and Changes

The Department received 43 different sets of comments on the proposed rule during the comment period. Two additional sets of comments were received on August 12, 2003, the day after the comment period ended, but in view of the relatively brief comment period (30 days), the Department has decided to accept those comments as well. The Department has considered all of the aforementioned 45 sets of comments, and summaries of the comments and the Department's responses follow.

Applicability and Use of Standards

The Department received a total of 24 comments relating to references to standards in the proposed rule. A change in the term ''safety and effectiveness standards,'' used in Section 25.3(c) of the proposed rule, to the industry accepted term ''technical standards,'' was suggested and has been implemented in Section 25.3(c) of the interim rule. A number of comments were made regarding the use of voluntary consensus technical standards and the advisability of ensuring that the Department provide for stakeholder participation in any standard development activities. The Department recognizes the advisability of such participation and has instituted a comprehensive program based on using the voluntary consensus process for the majority of its standard development activities. This process is designed to involve users, manufacturers, and private and public sector technical communities in all phases of standard development. The American National Standards Institute, numerous Standards Development Organizations, and the National Institute for Standards and Technology already have been actively involved in assisting the Department in accomplishing its standard development goals. Although the Department is vested with the authority to promulgate regulatory standards, the circumstances under which Department regulations governing anti-terrorism technologies are likely to be required are unusual. Therefore, the Department does not believe that there is a need for specific language about rulemaking with respect to standards.

One comment suggested postponing standard setting activities for two years in order to allow the market to stabilize. Other comments indicated a concern regarding possible prejudice against technologies that were not governed by formally accepted standards. The Department believes, however, that because of the rapidly evolving threat environment and the lack of basic standards for many classes of technologies, it is not in the best interest of the nation—and particularly of the emergency response community—to delay standard development activities. The Department also understands, however, that there is a continuing need for flexibility in the technical evaluation criteria under the SAFETY Act, and accordingly the Department will apply standards in SAFETY Act evaluations only to the extent that they are applicable to a particular technology and the circumstances of its proposed deployment. For those technologies without applicable standards (or with incomplete standards), additional methods of evaluation will be used, such as best practices, existing laboratory or field testing, etc. It will be highly desirable to use test information, where appropriate, from independent, accredited laboratories. The Department has also initiated a program to establish a network of certified labs that should address this need.

It will be important for SAFETY Act applicants to identify applicable standards that are appropriate to the specific operating environment and threat conditions for any potential anti-terrorism technology. The degree to which a proposed technology meets applicable standards will certainly be used to inform the technical evaluation process. However, technical effectiveness is only one facet of the criteria for issuance of a Designation or a Certification. Therefore, prior approval or certification by a United States Government agency (such as the Food and Drug Administration) will not be sufficient to form the basis for a SAFETY Act Designation or Certification per se, although such approval or certification might constitute relevant evidence of utility, effectiveness, or safety, and of course prior use of a technology by the United States Government is expressly relevant to the first criterion in Section 862(b)(1) of the SAFETY Act and the corresponding provision of the interim rule (§ 25.3(b)(1)).

Section 25.3(c) of the proposed rule stated that the Department will make available standards that are developed for anti-terrorism technologies. This service will apply only to potential regulatory criteria established by the Department. As noted by several commenters, many voluntary consensus technical standards are developed and owned by private sector entities. Where voluntary consensus standards are identified by the Department as being applicable to anti-terrorism

technologies, a summary of such standards may be published, along with a link to the appropriate site for the applicant to obtain or purchase the required or suggested standard. In preparing applications for SAFETY Act protections, however, applicants are encouraged not to limit themselves to standards previously promulgated or recognized by the Department, but rather to consider and reference any consensus technical standards that they believe to be applicable to technology.

Several standards development organizations suggested that voluntary consensus standards themselves be designated as qualified anti-terrorism technologies under the SAFETY Act. Although the Department believes it is unlikely that standards themselves will qualify for a Designation because it is unlikely that a standard will fall within the definition of ''qualified anti-terrorism technology'' in the Act, the Department will fully evaluate all applications for SAFETY Act protections received from Sellers of standards.

Scope of Required Insurance Coverage

Thirteen comments expressed concerns or confusion regarding the scope of required insurance coverage. Some commenters expressed uncertainty regarding the definition of the term ''Seller,'' the issue of who may be a defendant in the Federal cause of action prescribed in the SAFETY Act, and the nature of protection from liability afforded to entities other than the ''Seller'' in the manufacturing and distribution chains of the technology. In response, the Department has revised the definition of ''Seller'' in Section 25.9 of the interim rule in order to clarify that the ''Seller'' is the actual recipient of the Designation for a qualified anti-terrorism technology. The Department has also revised Section 25.4(a) of the interim rule to clarify that only the Seller is required to obtain the required liability insurance coverage.

Concern was expressed regarding the availability of insurance covering all of the parties specified in Section 864(a)(3) of the SAFETY Act and the corresponding provision in the interim rule (§ 25.4(c)). First, under the interpretation of Section 863 of the Act expressed by the Department in the preamble of the interim rule, (1) there is one exclusive Federal cause of action for claims relating to the deployment of a qualified anti-terrorism technology with respect to an act of terrorism, and (2) such cause of action may be brought only against the Seller, and only for injuries proximately caused by the Seller. Therefore, although other persons and entities must be covered by the required insurance coverage, the actuarial analyses of the insurance industry should focus mainly, if not exclusively, on the Seller's potential liability, which should facilitate the issuance of insurance policies. Moreover, in this context, the provisions of Section 864(a)(2) of the Act and the corresponding provision of the interim rule (§ 25.4(b)), which limit the required insurance to no more than the maximum amount reasonably available from private sources on the world market at prices and terms that will not unreasonably distort the sales price of Seller's anti-terrorism technologies (which the Department intends to interpret with regard to the effect of the insurance requirement on the price of the technology and ultimately on the demand for and deployment of the technology for anti-terrorism purposes), should be emphasized. It should also be noted that the Department has revised Section 25.4(a) of the interim rule to provide specifically for the possibility of self-insurance if the Under Secretary determines that insurance in appropriate amounts or of appropriate types is not available for a particular technology from third-party insurance carriers.

Term, Expiration, and Termination of Designation

Twenty-four comments were made suggesting that SAFETY Act Designations either should not expire or should have a longer duration (10–20 years) than provided for in the proposed rule (five to eight years). In response, the Department notes that qualification for a SAFETY Act Designation 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 rapid and unpredictable change. At the same time, the Department is very cognizant of the need for a guaranteed period of protection for successful SAFETY Act applicants in order to achieve the main goal of the Act, which is to facilitate the commercialization of needed anti-terrorism technologies. The Department believes that mandatory reconsideration of Designations after five to eight years provides a fair balancing of public and private interests.

Several comments suggested that SAFETY Act protections should have retroactive effect. There are two different senses of retroactivity that must be addressed. The first sense relates to the deployment of a technology. The Department believes that it would be inappropriate to apply SAFETY Act protections retroactively to deployments of a qualified anti-terrorism technology that occurred prior to the effective date of the Designation issued for such technology. The reasons are (1) there is no explicit authority to issue retroactive protections under the SAFETY Act, (2) a Designation with such retroactive effect would be potentially unlawful if it extinguishes an already accrued cause of action, (3) retroactive designation is not necessary to achieve, and does not further, the goals of the Act, and (4) there is no equitable method for determining the retroactivity of particular Designations. The Department believes that SAFETY Act protections should apply only to deployments of a qualified anti-terrorism technology that occur on or after the effective date of the Designation issued for such technology.

The second sense of retroactivity relates to the date of the sale of the qualified anti-terrorism technology by the Seller. The Department recognizes that, in some cases, technologies that qualify for SAFETY Act protections will have been sold by the Seller prior to the effective date of such protections. The Department believes that the date on which a technology was sold by a Seller, per se, is not necessarily relevant to the applicability of SAFETY Act protections to a deployment of the technology in defense against, response to, or recovery from an act of terrorism, provided that the technology is within the scope of a Designation and was originally sold by the Seller to which the Designation is issued. In other words, it might be appropriate for SAFETY Act protections to be applicable to any deployment of a qualified anti-terrorism technology that occurs on or after the effective date of the Designation issued for such technology even if such technology was originally sold by the Seller before the effective date of such Designation. The Department believes that any other interpretation would lead to anomalous and inequitable results. Therefore, provisions have been added to Sections 25.3(f), 25.4(f), 25.6(b), and 25.7(g) of the interim rule to clarify this issue, and in particular to require the Under Secretary to specify in each Designation and Certification the earliest date of the sale of the technology to which the protections will apply.

The Department notes that many qualified anti-terrorism technologies might be designed for continuous ''deployment'' (*e.g.*, sensors). The fact that a qualified anti-terrorism technology was sold and ''deployed'' prior to the effective date of an applicable Designation or Certification, or is, in a sense, continuously

''deployed,'' should not prevent such protections from applying to any deployment of such technology that occurs on or after the effective date of the applicable Designation or Certification in defense against, response to, or recovery from any act of terrorism.

Termination of a Designation Resulting From Significant Modification

Several comments expressed concern regarding Section 25.5(i) of the proposed rule, which provided for automatic termination if a designated technology is significantly modified or changed as defined in that provision. The concern was essentially that the standard for termination is too vague, although at least one commenter opposed automatic termination for any reason.

It is vital that the Department be able to ensure that technologies for which protections are granted are not changed in a way that will significantly affect their safety or effectiveness. The Department does not have the ability to monitor every change to a designated technology, however, and therefore the interim rule must place the burden on Sellers to submit proposed changes to the Department so that they may be properly evaluated.

That said, the Department agrees with one of the comments that suggested that only changes that significantly reduce the safety or effectiveness of the technology should be subject to automatic termination, and Section 25.5(i) of the interim rule has been revised accordingly. In addition, that Section has been revised to authorize the Under Secretary, in lieu of issuing a modified Designation, to issue a certificate to a Seller that certifies that a proposed change or modification to a technology does not significantly reduce its safety or effectiveness and reaffirms the applicability of the existing Designation to the technology. That option should enable the Under Secretary to respond swiftly to submissions of relatively minor changes. The Department strongly encourages holders of Designations to submit to the Under Secretary any proposed modifications or changes that could significantly reduce the safety or effectiveness of the designated technology.

One commenter wondered how the Department will evaluate a proposed change in advance when the factors to be evaluated would seem to require actual ''implementation'' of the change. The Department is confident that Sellers will have effective methods to evaluate the safety and effectiveness of changes to their technologies prior to actual commercialization, and the Department will take advantage of those same methods in its evaluation.

Confidentiality of Information

Seventeen commenters indicated a concern regarding the Department's ability to protect the confidentiality of information that is provided in an application. In particular, there is apprehension that the Freedom of Information Act (FOIA) protections might be inadequate to guarantee nondisclosure of an applicant's trade secrets or confidential business information. It was suggested that explicit protections similar to those available for source selection or procurement information under FAR section 3, or a declaration that all financial information provided is deemed voluntary, or both, be included in the interim rule.

The Department is committed to the protection of applicants' proprietary information to the fullest extent required or permitted by law. Although the interim rule does not establish any new special protections (such as those in section 3 of the FAR), there are multiple protections available for applicants' sensitive information. Those protections include the Trade Secrets Act (18 U.S.C. 1905), Exemption 1 (''national security'') of FOIA, and Exemption 4 (''privileged or confidential information'') of FOIA. In particular, Federal employees are subject to criminal penalties for unauthorized disclosure of information qualifying under Exemption 4 of FOIA. All contractors or other agents of the Secretary will be required to enter into nondisclosure agreements, and each will be examined on an Application-by-Application basis for potential conflicts of interest, before being granted access to any confidential information provided by applicants.

Services as Distinguished From Products

Fourteen comments expressed concerns that the language in the proposed rule did not make clear how certain provisions of the SAFETY Act will apply to services, as opposed to physical products. The Department recognizes that the Act applies equally to product-based technologies and service-based technologies.

The Department will evaluate services and products using the same seven non-exclusive criteria set forth in Section 862(b) and the corresponding provision in the interim rule (§ 25.3(b)), as required by the Act. These criteria include ''demonstrated substantial utility and effectiveness'' and ''studies * * * to assess the capability of the technology to substantially reduce risks of harm.'' Similarly, qualified Sellers of service-based technologies must satisfy the same post-Designation obligations as Sellers of products. These obligations include reporting insurance status, notifying the Secretary of any transfer or licensing of the designated technology, and applying for modification of a Designation prior to making any significant change to the designated technology. Appropriate revisions have been made to Section 25.5(i) and other provisions of the interim rule to clarify their applicability to services.

Transfer or licensing of Designations for products and, in particular, services may not be appropriate, since the identity and established expertise of the Seller is often be an integral basis for a Designation. That issue will be addressed in appropriate cases in individual Designations, as provided in Section 25.3(f) of the interim rule.

Determining the Required Amount of Insurance

A number of commenters discussed the potential difficulty of determining the amounts of insurance that must be carried to satisfy claims arising out of, relating to, or resulting from an act of terrorism with respect to which qualified anti-terrorism technologies have been deployed. Issues revolve around concern that most liability insurance is not purchased product-by-product, so that it might be difficult to estimate the ''price distortion'' caused by needing to insure a proposed new product or service. It was also suggested that there is a circular dependency between insurance costs and Designation: *i.e.*, the cost of insurance depends on the liability exposure, which depends on the content of the Designation (if any), which in turn depends on the cost of insurance. There was also concern expressed that insurance is not available at any price for certain technologies.

The Department is aware of the difficulties involved in quantifying the price impact of insuring (or self-insuring) against the specific potential liabilities addressed by the Act. The Department will rely on expert opinion and analysis in this area, as it will with technical determinations of safety and effectiveness. The Department will address the potential circularity issue by evaluating the need for SAFETY Act protections assuming the non-existence of such protections, and then setting the required amount of insurance by taking into account all relevant factors, including the cost and availability of

insurance coverage at different liability limitation levels.

Regarding potential unavailability of insurance for certain technologies, the Department notes that the granting of a Designation may render a previously uninsurable technology insurable through reduction of liability exposure. Where necessary to address unavailability of insurance, however, Designations may be granted that permit the insurance requirement to be satisfied by self-insurance up to a specified limit of liability. A new Section 25.4(f) and other provisions have been inserted in the interim rule to address this issue, as well as the continuing applicability of SAFETY Act protections after the expiration or termination of a Designation (which had been addressed in the proposed rule only in the preamble).

Clarification of Government Contractor Defense (GCD)

The precise nature and consequences of the GCD as applied by the Act were considered by 14 commenters to be unclear in the proposed rule. In particular, the interaction between the scope of the judicially derived GCD and the scope of the presumption defined in the Act was believed to be unclear.

As defined in the Act, the rebuttable presumption of the applicability of the GCD is accorded to any Seller who (1) has received Certification as described in Section 863(d), and (2) is the defendant in the Federal cause of action arising in Section 863(a). Pursuant to Section 863(d)(1), the presumption may only be overcome by evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information during the SAFETY Act application process.

The view of the Department is that the GCD protections afforded by the SAFETY Act to recipients of Certifications are similar to those affirmed by the courts in *Boyle* v. *United Technologies* and its progeny as of the date of the enactment of the SAFETY Act. In applying those protections, the Department believes that Congress intended that, for purposes of applying the GCD, courts presume that all of the legal and factual requirements for establishment of the GCD by a government contractor are met by the existence of an applicable SAFETY Act Certification.

The Department has added a new paragraph to Section 25.6 of the interim rule that corresponds to Section 863(d)(1) of the Act. Such new paragraph makes it clear that the presumption of the GCD will continue to apply in perpetuity to all deployments of technologies that receive a Certification, provided that the sale of the technology was consummated by the Seller prior to the expiration or termination of the applicable Certification.

Relationship of the SAFETY Act and Indemnification Under Public Law 85–804

Thirteen comments related to the relationship between SAFETY Act protections and indemnification under Public Law 85–804. The Department believes, however, that the language contained in part 8 of the ''Special Issues'' section of the preamble of the interim rule adequately explains such relationship, and makes it clear that eligibility for a SAFETY Act Designation does not preclude the granting of indemnification under Public Law 85–804.

Detailed Specification of the Seller, Technology, and Scope of a Designation

Twenty comments focused on the detailed specification of the Seller, technology, and scope of a Designation. Commenters suggested that there are advantages to the public, to industry, and to the application evaluation process in designating entire classes of technology, rather than designating each Seller of a technology individually.

The Department seeks to balance the need for rapid deployment of anti-terrorism technologies with the need for careful evaluation of each technology and the need to avoid uncertainty in the marketplace concerning which specific product or service deployments are protected by Designation. In general, Designations will be restricted in scope to a particular Seller, a specific product or service, and delineated types of deployment or application. This approach addresses the comment that it is beneficial to the public to be able to learn precisely which Sellers and which of their products/services have been designated, and for what scope of deployment. At some in the near future, as relevant standards are adopted and the body of ''substantially equivalent'' technologies increases, the Department will revisit the advisability of awarding broader Designations (''Block Designations'') to classes of technology.

Definition of ''Act of Terrorism''

Ten comments indicated a belief that the definition of ''act of terrorism'' in Section 865(2) of the Act (and in Section 25.9 of the interim rule) is ambiguous. One suggested that the definition coincide with other federal definitions of ''terrorism,'' such as the definition in 22 U.S.C. 2656f(d)(2). The Department notes that the definition of ''act of terrorism'' was prescribed by Congress in the SAFETY Act. The Department believes that the definition in the Act provides an appropriate degree of flexibility in the evolving threat environment, including the use of the broad term ''harm.'' Regarding the comment concerning whether acts that occur on foreign territory are covered by the definition, the Department's view is that the term ''act of terrorism,'' as defined, potentially encompasses acts that occur outside the territory of the United States. The basis for that view is that 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 statutory definition of ''act of terrorism'' has been added to Section 25.9 of the interim rule.

Determinations Not Subject to Review or Appeal

Five commenters observed that the SAFETY Act Designation and Certification processes are complex and that many apparently subjective assessments will be made during the evaluation process. They were concerned that the Secretary's decision is final, without recourse or appeal. Some commenters suggested that the Administrative Procedures Act (APA) requires a formal review as part of the process.

The Department is aware of the complexity of the review process and has made numerous allowances for exchange of information and concerns between evaluators and applicants at multiple points during the process, in order to clarify uncertainties and to give the applicant an opportunity to provide supplemental information and address issues. The Department believes that this interactive process provides sufficient recourse to applicants. The SAFETY Act is a discretionary authority accorded by Congress to the Secretary of Homeland Security in order 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 and application of the SAFETY Act criteria to the technology and the weighting of the criteria in each case. It would be inappropriate to provide for what would amount to the second-guessing of the Secretary's discretionary judgment by empowering another entity to substitute its own discretionary judgment for that of the Secretary.

SAFETY Act protections are not required to market any technology, and therefore the absence of a grant of protection under the SAFETY Act will not prevent any person or entity from doing business. The Department also notes that a SAFETY Act Designation is not a ''license required by law'' within the meaning of Section 558(c) of the APA, and thus is not covered by the APA.

Allowability of Insurance Costs

Four comments questioned whether the cost of maintaining the insurance required by a SAFETY Act Designation is an ''allowable cost'' under Federal contracting practices. The Department notes that each Federal procurement and contracting arrangement is unique to the Federal agency involved. When an applicant has questions regarding allowability for a specific case involving Federal procurements, the applicant should consult with the procuring agency and, if appropriate, with the applicant's legal counsel.

Burden of Proof With Regard to Evaluation Criteria

Three commenters asked, in essence, if the applicant bears the responsibility for demonstrating the applicability of each of the seven evaluation criteria. In particular, it was asked whether the applicant must establish the existence of an extraordinarily large or unquantifiable potential risk exposure (criterion 3), or the magnitude of risk exposure to the public if applicant's technology were not deployed (criterion 5). It was also asked whether applicants will bear the cost of scientific studies (criterion 6).

An application for a Designation or a Certification is a positive assertion on the applicant's part that the technology in question deserves special protections under the law in order to promote a public good. It is the applicant's responsibility to make a persuasive and defensible case. This will involve, at a minimum, submitting evidence that the technology satisfies the criteria in Section 862(b) of the SAFETY Act and the corresponding provision of the interim rule (§ 25.3(b)). To that end, an application that contains the most complete suite of supporting information regarding concrete evidence of proven or potential effectiveness will be more persuasive than an application that relies solely on the applicant's personal effectiveness estimates and *a priori* threat and liability assessments. Any evaluations needed to address the criteria will be the financial responsibility of the applicant.

Relationship of Designation and Certification Processes

Three comments addressed the linkage of the Designation and Certification processes. The Department believes that it is appropriate for these two aspects of the Act to remain closely aligned, and that the SAFETY Act indeed requires the issuance of a Designation for a technology to be a prerequisite (but not sufficient in itself) for issuance of a Certification. The same high standard of review will be applied to evaluations for Designations and Certifications, and a substantial amount of the information that is needed to evaluate applications for Designations is also integral to the Certification process (although there is additional information required to support the evaluation for a Certification). The Designation and the Certification are two separate protections with separate (but overlapping) criteria, and therefore they require two discrete application processes. The Department notes again, however, that applications for both protections may be considered in parallel, and that both protections may be granted simultaneously.

Multi-use Technologies and ''Specific Purpose''

Four commenters noted that the proposed rule stated that a technology must be ''designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying or deterring acts of terrorism * * *.'' They stated that the word ''specific,'' as used in this context, seems overly restrictive. They believe that this narrow reading could exclude from designation any product originally developed for another use.

The ''specific purpose'' clause was prescribed by Congress in Section 865(1) of the Act, and the Department does not have the authority to change that definition. The Department believes, however, that Congress did not intend for ''specific purpose'' to mean ''exclusive purpose.'' An applicant need only show that one specific purpose of the subject technology is to prevent, detect, identify, or deter acts of terrorism or limit the harm such acts might otherwise cause; it is irrelevant for purposes of the definition of ''qualified anti-terrorism technology'' that a technology might have other purposes or uses. Applications for SAFETY Act protections, and their component parts, should, of course, focus on the specific purpose(s) of the technology for which the applicant is seeking protection.

Expedited Reviews

Thirteen comments expressed a desire for the Department to provide expedited reviews for specific technologies based on various criteria. The approach of the Department will be to prioritize and expedite SAFETY Act applications in order to ensure that the highest risk vulnerabilities to the highest consequence threats are addressed first. In general, the Department will expedite reviews of SAFETY Act applications as its resources allow.

Reciprocal Waivers

Several comments stated that reciprocal waivers of the type described in the Act (reciprocal waivers of claims by the specified parties for losses sustained by them or their employees 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 customers, vendors, and suppliers may be unwilling to enter into such reciprocal agreements. The Department will not withhold or revoke a Designation based on the failure to obtain one or more required reciprocal waivers, provided that the Seller shows that it made diligent efforts in good faith to obtain such waivers.

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. Section 25.4(e) of the interim rule has been revised accordingly.

Mass Casualty Data

Four comments expressed concern over the use of mass casualty data. In particular, the proposed rule stated that the Secretary's inquiry concerning an application ''may involve * * * data and history regarding mass casualty losses.'' It was noted that, in the case of past mass tort settlements, such data may exist but be confidential. Questions were asked regarding whether providing such data (where it exists) would be mandatory for a Designation or a Certification, even when restricted by prior court-ordered confidentiality agreements, and whether special

protections would exist to prevent unauthorized disclosure.

The Department will not ask applicants to violate court ordered confidentiality agreements, but will expect that every reasonable effort will be made to extract relevant non-protected information or to provide equivalent information—*e.g.*, from industry aggregate data or summaries, etc.

Multiple Sellers

Questions were posed regarding whether it will be possible for joint ventures or other multi-party arrangements to receive SAFETY Act protections, and who will be responsible for obtaining insurance for such a multi-Seller Designation. A joint venture may take many forms. A joint venture that takes the form of a recognized business association with legal personality will be treated as a single Seller, and will be required to obtain insurance coverage itself.

As specified in the proposed rule, SAFETY Act protections may be issued to multiple Sellers (*e.g.*, a situation in which the owner of a technology and one or more of its licensees are to be covered by a single Designation). In that situation, the parties' respective obligations to obtain insurance will be specified in the Designation.

Discussion of Interim Rule

As part of the Homeland Security Act of 2002, Public Law 107–296, Congress enacted several liability protections for providers of 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 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 have been deployed. The Act does not limit liability for harms caused by anti-terrorism technologies when no act of terrorism has occurred.

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 individual technology, provided that Sellers will not 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 (Section 864(a)(2));
- A prohibition on joint and several liability for noneconomic damages, so that Sellers can only be liable for that percentage of noneconomic damages proportionate to their responsibility for the harm (§ 863(b)(2));
- A complete bar on punitive damages and prejudgment interest (§ 863(b)(1));
- A reduction of plaintiffs' recovery by amounts that plaintiffs received from ''collateral sources,'' such as insurance benefits or other government benefits (§ 863(c)); and
- A rebuttable presumption that the Seller is entitled to the ''government contractor defense'' (§ 863(d)).

The Act provides that these liability protections are conferred by two separate actions by the Secretary. The Secretary's designation of a technology as a ''qualified anti-terrorism technology'' confers all of the liability protections *except* the rebuttable presumption in favor of the government contractor defense. The presumption in favor of the government contractor defense requires an additional ''approval'' by the Secretary under Section 863(d) of the Act. In many cases, however, the designation and the approval can be conferred simultaneously.

Analysis

This preamble to the interim rule first addresses the two major aspects of the Act—the designation of qualified anti-terrorism technologies and the approval of technologies for purposes of the government contractor defense. Following that discussion, the preamble addresses specific issues regarding the interim rule and the Department's interpretation of the Act.

Designation of Qualified Anti-Terrorism Technologies

As noted above, the designation of a technology as a qualified anti-terrorism technology confers all of the liability protections provided in the 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 that must be considered to the extent that they are applicable to the 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. 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 based upon the particular technology at issue and the threats that the 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, after considering all of the relevant criteria, may conclude that a particular technology merits designation as a ''qualified anti-terrorism technology'' even if a particular criterion is 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 interim rule provides for designation as a qualified anti-terrorism technology for five to eight years.

The SAFETY Act applies to a very broad range of technologies, including products, services, software, and other forms of intellectual property, as long as the Secretary, as an exercise of discretion and judgment, determines that a technology merits designation under the statutory criteria. Further, as the statutory criteria suggest, a ''qualified anti-terrorism technology'' is not necessarily required to 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 Act also 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 technology at issue. Under § 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.'' Section 864(a)(1). The Act further provides that ''the Seller is not required to obtain liability insurance of more than the maximum amount of liability insurance reasonably available from private sources on the world market at prices and terms that will not unreasonably distort the sales price of Seller's anti-terrorism technologies'' (which the Department intends to interpret with regard to the effect of the insurance requirement on the price of the technology and ultimately on the demand for and deployment of the technology for anti-terrorism purposes). Section 864(a)(2).

The Secretary does not intend to set a ''one-size-fits-all'' numerical requirement regarding required insurance coverage for all technologies. Instead, as the Act suggests, the inquiry will be specific to each application and may involve an examination of several factors, including the following: the amount of insurance the Seller has previously maintained; the amount of insurance maintained by the Seller for other technologies or for the Seller's business as a whole; the amount of insurance typically maintained by sellers of comparable technologies; data and history regarding mass casualty losses; and the particular technology at issue. The Secretary will not require insurance beyond the point at which the cost of coverage would ''unreasonably distort'' the price of the technology. Once the Secretary concludes the analysis regarding the appropriate level of insurance coverage (which might include discussions with the Seller in appropriate cases), the Secretary will identify in a short certification a description of the coverage appropriate for the particular qualified anti-terrorism technology. If, during the term of the designation, the Seller would like to request reconsideration of that insurance certification due to changed circumstances or for other reasons, the Seller may do so. If the Seller fails to maintain coverage at the certified level during that time period, the liability protections of the Act will continue to apply, but the Seller's liability limit will remain at the certified insurance level. Such failure, however, will be regarded as a negative factor in the consideration of any future application by the Seller for renewal of the applicable designation, and perhaps in any other application by the Seller.

The Department solicits comment on the designation of qualified anti-terrorism technologies, including whether the five to eight year period is an appropriate length of time for such a designation.

Government Contractor Defense

The Act creates a rebuttable presumption that the government contractor defense applies to qualified anti-terrorism technologies ''approved by the Secretary'' in accordance with certain criteria specified in Section 863(d)(2). The government contractor defense is an affirmative defense that immunizes Sellers from liability for certain claims brought under Section 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 many of the requirements in the case law for 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 and 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 ''approval'' of technologies. Specifically, the Act provides that during the process of approval for the government contractor defense 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.'' Section 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.

The government contractor defense under *Boyle* and its progeny bars a broad range of claims. 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 that Congress incorporated 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 hard 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. Armey) (''[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 ''approval'' of a qualified anti-terrorism technology specifically for the purposes of the government contractor defense. This approval is a separate act from the Secretary's ''designation'' of a qualified anti-terrorism technology. Importantly, the Seller may submit applications for both designation as a qualified anti-terrorism technology and approval for purposes of the government contractor defense at the same time, and the Secretary may review and act upon both applications simultaneously. 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 of a qualified anti-terrorism technology. Specifically, the Act provides that during the process of approval for the government contractor defense 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.'' Section 863(d)(2). The Department believes that certain Sellers will be able to obtain the protections that come with designation as a qualified anti-terrorism technology even if they have not satisfied the requirements for the government contractor defense. Similarly, even if the applicability of the government contractor defense were rebutted under the test set forth in Section 863(d)(1) of the Act, the technology may still retain the designation and protections as a qualified anti-terrorism technology. Fraud or willful misconduct in the submission of information to the Department in connection with an application under the Act may result not only in rebuttal of the presumed application of the government contractor defense, but may also prompt the Department to refer the matter to the Department of Justice for pursuit of criminal or civil penalties.

The Department invites comment regarding the government contractor defense.

Specific Issues Regarding the Act and This Interim Rule

1. *Definition of Anti-Terrorism Technologies.* The Department recognizes that the universe of technologies that can be deployed against terrorism includes far more than physical products. Rather, the defense of the homeland will require deployment of a broad range of technologies that includes services, software, and other forms of intellectual property. Thus, consistent with Section 865 of the Act, Section 25.3(a) of the interim rule defines qualified anti-terrorism technologies very broadly to include ''any qualifying product, equipment, service (including support services), device, or technology (including information technology)'' that the Secretary, as an exercise of discretion and judgment, determines to merit designation under the statutory criteria.

2. *Development of New Technologies.* The Act's success depends not only upon encouraging Sellers to provide existing anti-terrorism technologies, but also upon encouraging Sellers to develop new and innovative technologies to respond to the ever-changing threats to the American people. The interim rule is thus designed to allow the Department to assist would-be Sellers during the invention, design, and manufacturing phases in two important respects. First, Section 25.3(h) of the proposal makes clear that the Department, within its discretion and where feasible, may provide feedback to inventors and manufacturers regarding whether proposed or developing anti-terrorism technologies might meet the qualification factors under the Act. The Department has developed a pre-application submission process in order to facilitate the procurement of such feedback. To be sure, the Department cannot provide advance designation, as some of the factors for the Secretary's consideration cannot be addressed in advance. The Department may, however, provide feedback regarding other factors, with the goal of giving potential Sellers some understanding of whether it might be advantageous to proceed with further development of the technology. Departmental feedback at the design, prototyping, or testing stage of development, to the extent feasible, may provide manufacturers with added incentive to commence and/or complete production of cutting-edge anti-terrorism technology that otherwise might not be produced or deployed in the absence of the risk and litigation management protections in the Act. The Department will perform these consultations with potential Sellers in a manner consistent with the protection of intellectual property and trade secrets, as discussed below.

Second, Section 25.3(g) of the interim rule recognizes that Federal, state, and local government agencies will often be the purchasers of anti-terrorism technologies. The Department recognizes that terms on which Sellers are able to provide anti-terrorism technologies to government agencies may vary depending on whether the technologies receive SAFETY Act coverage or not. The interim rule thus provides that the Department may coordinate SAFETY Act reviews with government agency procurements. The Department also intends to review SAFETY Act applications relating to technologies that are the subject of government agency procurements on an expedited basis.

The Department requests public comments regarding the best way for the Department to provide feedback to potential Sellers regarding SAFETY Act coverage and the best way for the Department to coordinate SAFETY Act review with agency procurements.

3. *Protection of Intellectual Property and Trade Secrets.* The Department believes that successful implementation of the Act requires that applicants' intellectual property interests and trade secrets remain protected in the application process and beyond. Toward that end, the Department will create an application and review process in which the Department maintains the confidentiality of an applicant's proprietary information. The Department notes that laws mandating disclosure of information submitted to the government generally contain exclusions or exceptions for such information. The Freedom of Information Act, for instance, provides specific exceptions for proprietary information submitted to Federal agencies.

4. *Evaluation of Scientific Studies; Consultation with Scientific and Technical Experts.* Section 862(b)(6) of the Act provides that, as one of many factors in determining whether to designate a particular technology under the Act, the Secretary shall consider evaluation of all scientific studies ''that can be feasibly conducted'' in order to assess the capability of the technology to substantially reduce the risks of harm. An important part of this provision is that it contemplates review only of such studies as can ''feasibly'' be conducted. The Department believes that the need to protect the American public by facilitating the manufacture and marketing of anti-terrorism technologies might render it infeasible to defer a designation decision until after every conceivable scientific study is completed. In many cases, existing

information (whether based on scientific studies, experience with the technology or a related technology, or other factors) might enable the Secretary to perform an appropriate assessment of the capability of the technology to reduce risks of harm. In other cases, even where less information is available about the capability of a technology to reduce risks of harm, the public interest in making the technology available as soon as practicable may render it infeasible to await the conduct of further scientific studies on that issue. In considering whether or to what extent it is feasible to defer a designation decision until additional scientific studies can be conducted, the Department will bring to bear its expertise concerning the protection of the American homeland and will consider the urgency of the need for the technology and other relevant factors and circumstances.

5. *''Exclusive Federal Jurisdiction'' and ''Scope'' of Insurance Coverage under Section 864(a)(3).* 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.'' Section 863(a)(2); *see also* section 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.'' Section 863(a)(1). The best reading of Section 863(a), and the reading the Department hereby adopts, is that (1) only one Federal cause of action exists for loss of property, personal injury, or death when a claim relates to the deployment (performance or non-performance) of the Seller's qualified anti-terrorism technology in defense against, response to, or recovery from an act of terrorism, and (2) such cause of action may be brought *only against the Seller.*

The exclusive Federal nature of this cause of action is evidenced in large part by the exclusive jurisdiction provision in Section 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.'' Section 863(a)(1) (emphasis added). Second, if the Seller of the qualified anti-terrorism technology at issue was 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 section 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.

The scope of Federal preemption of state laws is highly relevant to the Department's implementation of the Act, as the Department will have to determine the amount of insurance that Sellers must obtain. Accordingly, the Department seeks comment on that matter.

6. *Amount of Insurance.* The Act requires that Sellers obtain liability insurance ''of such types and in such amounts'' certified by the Secretary ''to satisfy otherwise compensable third-party claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed.'' Section 864(a)(1). However, the Act makes clear that Sellers are *not* required to obtain liability insurance beyond ''the maximum amount of liability insurance reasonably available from private sources on the world market at prices and terms that will not unreasonably distort the sales price of Seller's anti-terrorism technologies.'' Section 864(a)(2).

As explained above, the Department eschews any ''one-size-fits-all'' approach to the insurance coverage requirement. Instead, the Department construes the Act as contemplating the examination of several factors. Section 25.4(b) of the interim rule therefore sets forth a nonexclusive list of several factors that the Department may consider. These include the amount of insurance the Seller has previously maintained; the amount of insurance maintained by the Seller for other technologies or for the Seller's business as a whole; the amount of insurance typically maintained by sellers of comparable technologies; data and history regarding mass casualty losses; information regarding the amount of liability insurance offered on the world market; the particular technology at issue and its intended use; and the point at which the cost of coverage would ''unreasonably distort'' the price of the technology.

In the course of determining the amount of insurance required under the Act for a particular technology, the Department may consult with the Seller, the Seller's insurer, and others. While the decision regarding the amount of insurance required will generally be specific to each Seller or each technology, the Department recognizes that the incentive-based purposes of the Act may be furthered if the Department provides information to potential Sellers regarding the types and amounts of insurance that they will likely be required to obtain. Thus the Secretary may, where appropriate, give guidance to potential Sellers regarding the type and amounts of insurance that may be sufficient under the Act for particular

technologies or categories of technologies.

The Department also recognizes that the amount of insurance available at prices that will not unreasonably distort the price of the anti-terrorism technology may vary over time. Thus, the interim rule is written to give the Department flexibility to address fluctuating insurance prices by providing that, during the term of the designation, the Seller may request reconsideration of the insurance certification due to changed circumstances or other reasons.

The interim rule provides that the Seller shall certify on an annual basis that the Seller has maintained the insurance required by the Under Secretary's certification. It further provides that the Under Secretary may terminate the designation as a qualified anti-terrorism technology if the Seller fails to provide the certification or provides a false certification. Termination of the designation would mean that the Seller would not be able to sell the technology as a qualified anti-terrorism technology after the date of the termination. The Seller's failure to maintain the insurance also may adversely affect the Seller's ability to obtain a renewal of the designation for the technology, and may even adversely affect the Seller's ability to obtain future designations of ''qualified anti-terrorism technologies.'' Finally, a false certification may result in criminal or other penalties under existing laws.

The liability protections of the Act will continue to apply to technologies sold while the SAFETY Act designation was effective, regardless of whether the seller maintains the required insurance. This is necessary because the SAFETY Act protects not only the Seller, but also others in the manufacturing and distribution chains. For example, a buyer who purchases the technology while the SAFETY Act designation is still in effect should not be punished for the Seller's failure to maintain the insurance. The Seller, however, will face potential uninsured liability, because the Seller's liability limit will remain at the certified insurance level. This is because subsection (c) of Section 864 makes clear that the Seller's liability is capped at the amount of insurance ''*required*'' to be maintained under Section 864, rather than the amount of coverage actually obtained. The limitation of liability thus relates entirely to the amount of insurance required and makes no reference to whether such insurance is, in fact, maintained by the Seller.

The Department, as part of each certification, will specify the Seller or Sellers of the anti-terrorism technology for purposes of SAFETY Act coverage. The Department may, but need not, specify in the certification the others who are covered by the liability insurance required to be purchased by the Seller.

7. *Use of Standards.* Section 25.3(c) of the interim rule provides that the Under Secretary may issue technical standards for categories of anti-terrorism technologies, and that the Under Secretary may consider compliance with any such applicable standards in determining whether to grant a designation under the Act.

8. *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. Where applicable, the strong liability protections of the SAFETY Act should, in most circumstances, make it unnecessary to provide indemnification to Sellers. The Department recognizes, however, that there might be, in some limited circumstances, technologies or services with respect to which both SAFETY Act coverage and indemnification might be warranted. *See* 148 Cong. Rec. E2080 (statement by Rep. Armey) (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 recently 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 and 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.''

Application of Various Laws and Executive Orders to This Interim Rulemaking

Executive Order 12866—Regulatory Planning and Review

The Department has examined the economic implications of this interim 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.

The Department did not receive any comments on our economic analysis.

The Department concludes that this interim 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), and it raises novel legal and policy issues under Section 3(f)(4). The Department concludes, however, that this interim 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 this interim rule to have a large impact on the public.

Need for the Regulation and Market Failure

This regulation 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 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.'' TRIA § 101(b)(2). This interim rulemaking addresses a similar concern, to the extent that potential technology developers are unable to efficiently insure 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 to efficiently 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 this interim rule are designed to meet this goal; they will provide certain liability protection from lawsuits and consequently will increase the likelihood that businesses will pursue important technologies that may not be pursued without this protection.

Costs and Benefits to Technology Development Firms

Since this interim rulemaking puts in place an additional voluntary option for technology developers, the expected direct net benefits to firms of this interim rulemaking will be positive; companies presumably will not choose to pursue the designation of ''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. The Department invites comments on these issues.

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 costs. Please see the accompanying PRA analysis for an estimate of these costs.

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 only consider benefits and costs specifically due to the implementation of the interim rule and not costs that would have been incurred by companies absent any interim 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 this interim rule for firms.

The wording 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 interim 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 this interim 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 this interim rule to firms. This change will most likely be a shift back 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 interim rulemaking will lead to greater market entry, which will generate surplus for both technology firms and insurers. Again, this market is still in development, and the Department solicits comments on exactly how to predict the effect of this interim rulemaking on technology development.

Costs and Benefits to Insurers

The Department has little information on the future structure of the terrorism risk insurance market, and how this interim rulemaking 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 from insurers to technology firms. On the other hand, this type of intervention should serve to increase the surplus of insurers by making some types of insurance products possible that would have been prohibitive to customers or impossible for insurers to design in the absence of this interim rulemaking. The Department is interested in public comment on any possible negative or positive impacts to insurers caused by the SAFETY Act and this interim rulemaking, and whether these impacts would result in transfers within this market or an efficiency change not captured by another party. We encourage commenters to be as specific as possible.

Costs and Benefits to the Public

The benefits to the public of this interim rulemaking are very difficult to put in dollar value terms since its ultimate objective is the development of new technologies that will help prevent or limit the damage from terrorist attacks. It is not possible to even 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 interim 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 too strong or prohibitive, for the reasons mentioned above. The Department tentatively concludes that this interim rule will have positive net benefits to the public, since it serves to strike a better balance between consumer protection and technological development. The Department welcomes comments informing this tradeoff argument, and public input on whether this interim rulemaking does strike the correct balance.

Collection of Information

Paperwork Reduction Act of 1995

This interim rule includes collection of information under the Paperwork Reduction Act of 1995 (Paperwork Reduction Act) (44 U.S.C. 3501–3520). As defined in 5 CFR 1320(c), ''collection of information'' comprises reporting, recordkeeping, monitoring, posting, labeling, and other similar actions. The title and description of the information collections, a description of those who must collect the information, and an estimate of the total annual burden follow. The estimate covers the time for reviewing instructions, searching existing sources of data, gathering and maintaining the data needed, and completing and reviewing the collection.

The Department submitted the following information collection requests to the Office of Management and Budget (OMB) for emergency review with an expiration of six months from the date of publication of this interim rule in accordance with procedures of the Paperwork Reduction Act of 1995. The proposed information collection will be published to obtain comments from the public and affected agencies.

The Department requests comments on at least the following four points:

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

(2) The accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

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

(4) The burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.*, permitting electronic submission of responses.

For the purpose of each analysis described below and associated with each collection of information, the Department assumes a loaded labor rate of the personnel preparing each collection of information to be $100 per hour. The Department does not have sufficient information to provide a known number of applicants or submitters of information. All numbers are estimates.

This rule requires persons to conduct safety, effectiveness, utility, and hazard analyses and provide them to the Under Secretary in the course of applying for Designation of qualified anti-terrorism technology. We do not have quantified estimates of the impact of this provision, but we expect that much of the safety, effectiveness, utility, and hazard analysis activity will already take place in the normal course of technology development, since those matters are fundamental characteristics of a product. The Department acknowledges considerable uncertainty in these estimates, but even if the estimates were considerably higher, this does not represent a large investment by firms relative to overall development costs.

Overview of Requests for Collection of Information

(a) Collection of Information Form No. DHS–S&T–I–SAFETY–001.

(1) *Type of Information Collection:* New Collection.

(2) *Title of the Form/Collection:* Pre-Application for Designation of Qualified Anti-terrorism Technology.

(3) *Agency form numbers and applicable component sponsoring the collection:* Form Number: DHS–S&T–I–SAFETY–001, Directorate of Science and Technology, Department of Homeland Security.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* Primary: Sellers and potential Sellers of qualified anti-terrorism technology. Abstract: The Pre-Application Form for Designation of Qualified Anti-Terrorism Technology will be used to provide information to the Under Secretary for Science and Technology of the Department of Homeland Security in determining whether Sellers pre-qualify for risk and litigation management protections under the SAFETY Act.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* 1,000 applicants annually; 14 to 72 hours per application.

(6) *An estimate of the total public burden (in hours) associated with the collection:* 14,000 to 72,000 hours.

(b) Collection of Information Form No. DHS–S&T–I–SAFETY–002.

(1) *Type of Information Collection:* New Collection.

(2) *Title of the Form/Collection:* Application for Designation of Qualified Anti-Terrorism Technology.

(3) *Agency form numbers and applicable component sponsoring the collection:* Form Number: DHS–S&T–I–SAFETY–002, Directorate of Science and Technology, Department of Homeland Security.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* Primary: Sellers and potential Sellers of qualified anti-terrorism technology. Abstract: The Application Form for Designation of Qualified Anti-Terrorism Technology will be used to provide information to the Under Secretary for Science and Technology of the Department of Homeland Security in determining whether Sellers qualify for risk and litigation management protections under the SAFETY Act.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* 1,000 applicants annually; 36 to 180 hours per application.

(6) *An estimate of the annual total public burden associated with the collection:* 36,000 to 180,000 hours.

(c) Collection of Information Form No. DHS–S&T–I–SAFETY–003.

(1) *Type of Information Collection:* New Collection.

(2) *Title of the Form/Collection:* Application of Transfer of Designation.

(3) *Agency form numbers and applicable component sponsoring the collection:* Form Number: DHS–S&T–I–SAFETY–003, Directorate of Science and Technology, Department of Homeland Security.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* Primary: Sellers of qualified anti-terrorism technology. Abstract: The Application Form for Transfer of Designation will be used by Sellers to notify the Under Secretary for Science and Technology of the Department of Homeland Security of a transfer of Designation.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* 250 to 500 applicants annually, 15 to 30 minutes per application.

(6) *An estimate of the annual total public burden (in hours) associated with the collection:* 250 hours.

(d) Collection of Information Form No. DHS–S&T–I–SAFETY–004.

(1) *Type of Information Collection:* New Collection.

(2) *Title of the Form/Collection:* Notice of License of Qualified Anti-Terrorism Technology.

(3) *Agency form numbers and applicable component sponsoring the collection:* Form Number: DHS–S&T–I–SAFETY–004, Directorate of Science and Technology, Department of Homeland Security.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* Primary: Sellers of qualified anti-terrorism technology. Abstract: The Notice of License of Qualified Anti-Terrorism Technology.

Application Form for Transfer of Designation will be used by Sellers to notify the Under Secretary for Science and Technology of the Department of Homeland Security of its license of the right to manufacture, use or sell Designated technology.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* 250 to 500 applicants annually; fifteen to thirty minutes per application.

(6) *An estimate of the annual total public burden (in hours) associated with the collection:* 250 hours.

(e) Collection of Information Form No. DHS–S&T–I–SAFETY–005.

(1) *Type of Information Collection:* New Collection.

(2) *Title of the Form/Collection:* Notice of License of Approved Technology.

(3) *Agency form numbers and applicable component sponsoring the collection:* Form Number: DHS–S&T–I–SAFETY–005, Directorate of Science and Technology, Department of Homeland Security.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* Primary: Sellers of approved anti-terrorism technology. Abstract: The Form for Notice of License of Approved Anti-Terrorism Technology will be used by Sellers to notify the Under Secretary for Science and Technology of the Department of Homeland Security of the right to manufacture and sell approved technology.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* 250 to 500 applicants annually; fifteen to thirty minutes per application.

(6) *An estimate of the annual total public burden (in hours) associated with the collection:* 250 hours.

(f) Collection of Information Form No. DHS–S&T–I–SAFETY–006.

(1) *Type of Information Collection:* New Collection.

(2) *Title of the Form/Collection:* Application for Modification of Designation.

(3) *Agency form numbers and applicable component sponsoring the collection: Form Number:* DHS–S&T–I–SAFETY–006, Directorate of Science and Technology, Department of Homeland Security.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* Primary: Sellers of qualified anti-terrorism technology. Abstract: The Application Form for Modification of Designation will be used by Sellers to apply to the Under Secretary for Science and Technology of the Department of Homeland Security for approval of modification of a designation of Qualified Anti-Terrorism Technology.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* 250 applicants annually; 10 to 20 hours per application.

(6) *An estimate of the annual total public burden (in hours) associated with the collection:* 5,000 hours.

(g) Collection of Information Form No. DHS–S&T–I–SAFETY–007.

(1) *Type of Information Collection:* New Collection.

(2) *Title of the Form/Collection:* Application for Renewal of Certification of an Approved Product for Homeland Security.

(3) *Agency form numbers and applicable component sponsoring the collection:* Form Number: DHS–S&T–I–SAFETY–007, Directorate of Science and Technology, Department of Homeland Security.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* Primary: Sellers of qualified anti-terrorism technology. Abstract: The Application Form for Renewal of Certification of an Approved Product for Homeland Security will be used by Sellers to request renewal of Certification of an approved product for Homeland Security to the Under Secretary for Science and Technology of the Department of Homeland Security.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* 250 to 500 applicants annually; fifteen to thirty minutes per application.

(6) *An estimate of the annual total public burden (in hours) associated with the collection:* 250 hours.

(h) *Additional Information:* If additional information is required on any of these forms, contact: Directorate of Science and Technology, SAFETY Act/room 4320, Department of Homeland Security, Washington, DC 20528.

(i) *Submission of Comments on the Collection of Information:* If you submit comments on the collection of information, submit them both to OMB and to the Docket Management Facility where indicated under addresses, by the date under Dates.

(j) *Valid OMB Control Document:* You need not respond to a collection of information unless it displays a currently valid control document from OMB.

Regulatory Flexibility Act

The Regulatory Flexibility Act requires the Department to determine whether this interim 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 interim rulemaking will impose a significant financial impact on them. In fact, we believe this interim rule will be a benefit to technology development businesses, especially small businesses, by presenting 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 interim 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.

To the extent that demand for insurance falls, however, insurers may be adversely impacted by this interim 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 interim rulemaking on insurers is ambiguous but could very well be positive. We also expect that this interim rulemaking will affect relatively few firms and relatively few insurers either positively or negatively, as this appears to be a specialized industry. Therefore, we preliminarily certify this notice of interim rulemaking will not have a significant impact on a substantial number of small entities, and we request comments on this certification.

Unfunded Mandates Reform Act of 1995

This interim 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.

Small Business Regulatory Fairness Act of 1996

As noted above, the Department has tentatively determined that this interim rule would not qualify as a ''major rule'' as defined by section 804 of the Small Business and Regulatory Enforcement Act of 1996.

Executive Order 13132—Federalism

The Department of Homeland Security does not believe this interim 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 this interim rule to the extent that they are purchasers of qualified anti-terrorism technologies. The Department requests comment on the federalism impact of this Interim rule. In particular, the Department seeks comment on whether this interim rule will raise significant federalism implications and, if so, what is the nature of those implications.

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 Chapter I is amended by adding part 25 to read as follows:

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

Sec.
25.1 Purpose.
25.2 Delegation.
25.3 Designation of qualified anti-terrorism technologies.
25.4 Obligations of seller.
25.5 Procedures for designation of qualified anti-terrorism technologies.
25.6 Government contractor defense.
25.7 Procedures for certification of approved products for homeland security.
25.8 Confidentiality and protection of intellectual property.
25.9 Definitions.

Authority: Subtitle G, 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, Subtitle G of Title VIII of Public Law 107–296 (''the SAFETY Act'' or ''the Act'').

§ 25.2 Delegation.

All of the Secretary's responsibilities, powers, and functions under the SAFETY Act may be exercised by the Under Secretary for Science and Technology of the Department of Homeland Security (''the Under Secretary'') or the Under Secretary's designees.

§ 25.3 Designation of qualified anti-terrorism technologies.

(a) *General.* The Under Secretary may designate as a qualified anti-terrorism technology for purposes of protections set forth in Subtitle G of Title VIII of Public Law 107–296 any qualifying product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause.

(b) *Criteria to be considered.* In determining whether to grant the designation under paragraph (a) (a ''Designation''), the Under Secretary may exercise discretion and judgment in interpreting and weighting the following criteria in each case:

(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 6 U.S.C. 441–444 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) Any other factor that the Under Secretary may consider to be relevant to the determination or to the homeland security of the United States.

(c) *Use of standards.* From time to time the Under Secretary may develop, issue, revise, and adopt technical standards for various categories of anti-terrorism technologies. Such standards will be published by the Department at *http://www.dhs.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. Compliance with any such standards that are applicable to a particular anti-terrorism technology may be considered before any Designation will be granted for such technology under paragraph (a) of this section; in such cases, the Under Secretary may consider test results produced by an independent laboratory or other entity engaged to test or verify the safety, utility, performance, or effectiveness of such technology.

(d) *Consideration of substantial equivalence.* In determining whether a particular technology satisfies the criteria in paragraph (b) and complies with any applicable standards referenced in paragraph (c), the Under Secretary may take into consideration evidence that the technology is substantially equivalent to other, similar technologies (''predicate technologies'') that have been previously 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 technological characteristics as the predicate technology.

(e) *Duration and depth of review.* Recognizing the urgency of certain security measures, the Under Secretary will make a judgment regarding the duration and depth of review appropriate for a particular technology. This review will include submissions by the applicant for SAFETY Act coverage, along with information that the Under Secretary can feasibly gather from other sources. 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 that 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 in order to assess the capability of the technology to substantially reduce risks of harm. Such studies may, in the Under Secretary's discretion, include:

(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 or her expertise concerning the protection of the security of the American homeland and will consider the urgency of the need for the technology.

(f) *Content of Designation.* A Designation shall specify the technology, the Seller(s) of the technology, and the earliest date of sale of the technology to which the Designation shall apply (which shall be determined by the Under Secretary in his or her discretion, and may be prior to, but shall not be later than, the effective date of the Designation). The Designation may, but need not, also specify others who are required to be covered by the liability insurance required to be purchased by the Seller. The Designation shall include the Under Secretary's certification required by § 25.4(h). The Designation may also include such other specifications as the Under Secretary may deem to be appropriate, including, but not limited to, specific applications of the technology, materials or processes required to be used in producing or using the technology, restrictions on transfer or licensing, and training and instructions required to be provided to persons involved in the deployment of the technology. Failure to specify a covered person or entity in a Designation will not preclude application of the Act's protections to that person or entity.

(g) *Government procurements.* The Under Secretary may coordinate a SAFETY Act review in connection with a Federal, state, or local government agency procurement of an anti-terrorism technology in any manner he or she deems appropriate and consistent with the Act and other applicable laws.

(h) *Pre-application consultations.* To the extent that he or she deems it appropriate, the Under Secretary may consult with potential SAFETY Act applicants regarding the need for or advisability of particular types of anti-terrorism technologies, although no pre-approval of any particular technology may be given. Such potential applicants may request such consultations through the Pre-Application process set forth in the SAFETY Act Application Kit. The confidentiality provisions in § 25.8 shall be applicable to such consultations.

§ 25.4 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. Notwithstanding the foregoing, if the Under Secretary determines that insurance in appropriate amounts or of appropriate types is not available for a particular technology, the Under Secretary may authorize a Seller to self-insure and prescribe the amount and terms of the Seller's liability in the applicable Designation, which amount and terms shall be such as will not unreasonably distort the sales price of the Seller's anti-terrorism technology. The Under Secretary may request at any time (before or after the insurance certification process established under this section) that the Seller or any other provider of 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 the requirements of this section.

(b) *Maximum Amount.* For the total claims related to one act of terrorism, in determining the required amounts and types of liability insurance that the Seller will be required to obtain, the Under Secretary shall 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 at prices and terms that will not unreasonably distort the sales price of the Seller's anti-terrorism technology. The Under Secretary will determine the amount of liability insurance required for each technology, or, to the extent feasible and appropriate, a particular group of technologies. The Under Secretary or his designee may find that—notwithstanding the level of risk exposure for a particular technology, or group of technologies—the maximum amount of liability insurance from private sources on the world market is set at a price or contingent on terms that will unreasonably distort the sales price of a Seller's technology, thereby necessitating liability insurance coverage below the maximum amount available. 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;

(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; and

(9) In the case of a Seller seeking approval to self-insure, the factors described in 48 CFR 28.308(d).

(c) *Scope of coverage.* Liability insurance required to be obtained (or self-insurance required) 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.

(d) *Third party claims.* Any liability insurance required to be obtained (or self-insurance required) 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, if the Seller has used diligent efforts in good faith to obtain all required reciprocal waivers, then 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) *Extent of liability.* 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 in accordance with the applicable Designation and such claims result or may result in loss to the Seller, whether for compensatory or punitive damages or for contribution or indemnity, shall not be in an amount greater than the limits of liability insurance coverage required to be maintained by the Seller under this Section, or, in the case of a Seller authorized by the Under Secretary to self-insure pursuant to this Section, shall not be in an amount greater than the liability limit prescribed by the Under Secretary in the applicable Designation.

(1) In addition, in any action brought under Section 863 of the Act for damages:

(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.

(2) Without prejudice to the authority of the Under Secretary to terminate a Designation pursuant to paragraph (h) of this Section, such liability limitations and reductions shall apply in perpetuity to all deployments of a qualified anti-terrorism technology that occur on or after the effective date of the Designation applicable to such technology in defense against, response to, or recovery from any act of terrorism, regardless of whether any liability insurance coverage required to be obtained by the Seller is actually maintained or not, 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 Designation (which shall be determined by the Under Secretary in his or her discretion, and may be prior to, but shall not be later than, such effective date) and prior to the expiration or termination of such Designation.

(g) *Information to be submitted by the Seller.* As part of any application for a Designation, the Seller shall provide a statement, executed by a duly authorized representative of the Seller, of all 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;

(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 terror;

(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;

(8) Any limitations on such liability insurance; and

(9) In the case of a Seller seeking approval to self-insure, all of the information described in 48 CFR 28.308(a)(1) through (10).

(h) *Under Secretary's certification.* For each qualified anti-terrorism technology, the Under Secretary shall certify the amount of insurance required under Section 864 of the Act. The Under Secretary shall include the certification under this section as a part of the applicable Designation. The certification may specify a period of time for which the certification will apply. The Seller of a qualified anti-terrorism technology may at any time petition the Under Secretary for a revision or termination of the certification under this section. The Under Secretary or his designee may at any time request information from the Seller regarding the insurance maintained by the Seller or the amount of insurance available to the Seller.

(i) *Seller's continuing obligations.* Within 30 days after the Under Secretary's certification required by paragraph (h), and within 30 days after each subsequent anniversary of the issuance of a Designation, the Seller shall certify to the Under Secretary that the Seller has maintained the insurance required by such certification. The Under Secretary may terminate a Designation if the Seller fails to provide

the certification required by this paragraph or provides a false certification. The Under Secretary may also consider such failure to provide the certification or provision of a false certification when reviewing future applications from the same Seller. The Seller must also notify the Under Secretary of any changes in types or amounts of liability insurance coverage for any qualified anti-terrorism technology.

§ 25.5 Procedures for designation of qualified anti-terrorism technologies.

(a) *Application procedure.* Any Seller seeking a designation shall submit information supporting such request to the Assistant Secretary for Plans, Programs, and Budget of the Department of Homeland Security Directorate of Science and Technology (''the Assistant Secretary''), or such other official of such Directorate as may be designated from time to time by the Under Secretary. The Under Secretary shall make application forms available at *http://www.dhs.gov* and by mail upon request sent to: Directorate of Science and Technology, SAFETY Act/room 4320, Department of Homeland Security, Washington, DC 20528.

(b) *Initial notification.* Within 30 days after receipt of an Application for a Designation, the Assistant Secretary or his or her 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 Assistant Secretary or his or her designee will review each complete Application and any included supporting materials. In performing this function, the Assistant Secretary or his or her 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 nonfederal entity;

(4) Perform studies or analyses of the technology or the insurance market for such technology; and

(5) Seek information from insurers regarding the availability of insurance for such technology.

(d) *Recommendation of the Assistant Secretary.* (1) Within 90 days after receipt of a complete Application for a Designation, the Assistant Secretary shall make one of the following recommendations to the Under Secretary regarding such Application:

(i) That the Application be approved and a Designation be issued to the Seller;

(ii) That the Seller be notified that the technology is potentially eligible for a Designation, but that additional specified information is needed before a decision may be reached; or

(iii) That the Application be denied.

(2) If approval is recommended, the recommendation shall include a recommendation regarding the certification required by § 25.4(h). The Assistant Secretary may extend the time period beyond 90 days upon notice to the Seller; the Assistant Secretary is not required to provide a reason or cause for such extension.

(e) *Action by the Under Secretary.* Within 30 days after receiving a recommendation from the Assistant Secretary pursuant to paragraph (d) of this section, the Under Secretary shall take one of the following actions:

(1) Approve the Application and issue an appropriate Designation to the Seller, which shall include the certification required by §25.4(h);

(2) Notify the Seller 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 Seller in writing of such decision. The Under Secretary may extend the time period beyond 30 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.

(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 based upon the technology) commencing on the date of issuance. At any time commencing two years prior to the expiration of a Designation, the Seller may apply for renewal of the Designation. The Under Secretary shall make the application form for renewals available at *http://www.dhs.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) *Transfer of Designation.* (1) Except as may be restricted by the terms and conditions of a Designation, any Designation may be transferred and assigned to any other person or 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 or 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:

(i) 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.dhs.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), and

(ii) the transferee complies with all applicable provisions of the SAFETY Act, this Part, and the relevant Designation as if the transferee were the Seller.

(2) 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.

(h) *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 or entity to which the 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 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.dhs.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.

(i) *Termination of Designation resulting from significant modification.*

A Designation shall terminate automatically, and have no further force or effect, if the designated qualified anti-terrorism technology is significantly changed or modified. A significant change or modification in the technology is one that could significantly reduce the safety or effectiveness of the technology. This could include, in the case of a device, a significant change or modification in design, material, chemical composition, energy source, manufacturing process, or purpose for which it is to be sold, and in the case of a service, a significant change or modification in methodology, procedures, or purpose for which it is to be sold. If a Seller is planning a change or modification to a designated technology, such Seller may apply for a corresponding modification of the applicable Designation in advance of the implementation of such modification. Application for such a modification must be made using the ''Application for Modification of Designation'' form issued by the Under Secretary. The Under Secretary shall make this application form available at *http://www.dhs.gov* and by mail upon request sent to: Directorate of Science and Technology, SAFETY Act/room 4320, Department of Homeland Security, Washington, DC 20528. Changes or modifications will be evaluated at a minimum with reference to the description of the technology and its purposes as provided in the Seller's application and with reference to what was designated in the applicable Designation. In lieu of issuing a modified Designation in response to such an application, the Under Secretary may elect to issue a certificate to the Seller certifying that the submitted changes or modifications are not significant within the meaning of this paragraph (i) and that the Seller's existing Designation continues to be applicable to the changed or modified technology.

§ 25.6 Government contractor defense.

(a) *Criteria for certification.* The Under Secretary may certify 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 grant such certification, the Under Secretary or his or her 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 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 or entity, and may consider test results produced by an independent laboratory or other person or 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 §§ 25.6 and 25.7 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 evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Assistant Secretary during the course of the Assistant Secretary's consideration of such technology under this subsection. This presumption of the government contractor defense shall apply regardless of whether the claim against the Seller arises from a sale of the product to Federal Government or non-Federal Government customers. 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 § 25.7) that occur on or after the effective date of the Certification applicable to such technology in defense against, response to, or recovery from any act of terrorism, 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 or her 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.

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

(a) *Application procedure.* A Seller seeking certification of anti-terrorism technology as an Approved Product for Homeland Security under §25.6 (a ''Certification'') shall submit information supporting such request to the Assistant Secretary. The Under Secretary shall make application forms available at *http://www.dhs.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 Seller has also filed an application for designation of qualified anti-terrorism technology for the same technology. The two applications may be filed simultaneously and may be reviewed simultaneously.

(b) *Initial notification.* Within 30 days after receipt of an Application for a Certification, the Assistant Secretary or his or her 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 Assistant Secretary or his or her designee will review each complete Application for a Certification and any included supporting materials. In performing this function, the Assistant Secretary or his or her 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 nonfederal entity; and

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

(d) *Recommendation of the Assistant Secretary.* (1) Within 90 days after receipt of a complete Application for a Certification, the Assistant Secretary shall make one of the following recommendations to the Under Secretary regarding such Application:

(i) That the Application be approved and a Certification be issued to the Seller;

(ii) That the Seller be notified that the technology is potentially eligible for a Certification, but that additional specified information is needed before a decision may be reached; or

(iii) That the Application be denied.

(2) The Assistant Secretary may extend the time period beyond 90 days upon notice to the Seller; the Assistant Secretary is not required to provide a reason or cause for such extension.

(e) *Action by the Under Secretary.* (1) Within 30 days after receiving a

recommendation from the Assistant Secretary pursuant to paragraph (d) of this section, 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 beyond 30 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.

(f) *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 under section 25.3.

(g) *Content and term of certification; renewal.* A Certification shall specify the technology, the Seller(s) of the technology, and the earliest date of sale of the technology to which the Certification shall apply (which shall be determined by the Under Secretary in his or her discretion, and may be prior to, but shall not be later than, the effective date of the Certification). The Certification may also include such other specifications as the Under Secretary may deem to be appropriate, including, but not limited to, specific applications of the technology, materials or processes required to be used in producing or using the technology, restrictions on transfer or licensing, and training and instructions required to be provided to persons involved in the deployment of the technology. 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.

(h) *Application of Certification to licensees.* Any certification shall apply to any other person or entity to which the Seller licenses (exclusively or nonexclusively) the right to manufacture 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.dhs.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.

(i) *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.

(j) *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 of Homeland Security.

§ 25.8 Confidentiality and protection of intellectual property.

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 protocols for maintenance and use of information submitted to the Department under the SAFETY Act and this Part. Such protocols shall, among other things, ensure that the Department will utilize all appropriate exemptions from the Freedom of Information Act.

§ 25.9 Definitions.

Act of Terrorism—The term ''act of terrorism'' means any act that—

(1) Is unlawful;

(2) Causes harm to a person, property, or entity, in the United States, or in the case of a domestic United States air carrier or a United States-flag vessel (or a vessel based principally in the United States on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), in or outside the United States; and

(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.

Assistant Secretary—The term ''Assistant Secretary'' means the Assistant Secretary for Plans, Programs, and Budget of the Department of Homeland Security Directorate of Science and Technology, or such other official of such Directorate as may be designated from time to time by the Under Secretary.

Certification—The term ''Certification'' means (unless the context requires otherwise) a certification 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'' of a Seller means any person or entity with whom or with which the Seller has entered into a contract 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 a designation of a qualified anti-terrorism technology under the SAFETY Act issued by the Under Secretary under authority delegated 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.

Physical harm—The term ''physical harm'' as used in the Act shall mean a physical injury to the body 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 (QATT)—The term '''qualified anti-terrorism technology''' means any product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, for which a Designation has been issued under this Part.

SAFETY Act or Act—The term ''SAFETY Act'' or ''Act'' means the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, enacted as Subtitle G of Title VIII of the Homeland Security Act of 2002, Public Law 107–296.

Seller—The term ''Seller'' means any person or entity to whom or to which (as appropriate) a Designation has been issued under this Part (unless the context requires otherwise).

Under Secretary—The term ''Under Secretary'' means the Under Secretary for Science and Technology of the Department of Homeland Security.

Dated: October 10, 2003.

Tom Ridge,

Secretary of Homeland Security.

[FR Doc. 03–26217 Filed 10–10–03; 4:15 pm]

BILLING CODE 4410–10–P