

**Department of Homeland Security
SAFETY Act Application Kit**

October 2003

Registration

Pre-Application

Application for Designation as Qualified Anti-Terrorism Technology

Application for Certification as an Approved Product for Homeland Security

FOREWORD

We are pleased to release the October 2003 version of the *Department of Homeland Security SAFETY Act Application Kit*. The kit provides you with all of the necessary guidelines for developing and submitting an Application for a Designation or a Certification under the SAFETY Act.

As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted the SAFETY Act to provide “risk management” and “litigation management” protections for Sellers of qualified anti-terrorism technologies and others in the supply and distribution chain. The aim of the Act is to encourage the development and deployment of anti-terrorism technologies that will substantially enhance the protection of the nation. Specifically, the SAFETY Act 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. It also confers other benefits. Although there are many technologies that are important to protecting our homeland, the SAFETY Act “Designation” and “Certification” are designed to support effective technologies aimed at preventing, detecting, identifying, or deterring acts of terrorism, or limiting the harm that such acts might otherwise cause, and which also meet other prescribed criteria.

If you are a Seller of a potential anti-terrorism technology and wish to be awarded SAFETY Act protections, you must formally apply to the Department using the forms provided by DHS, furnish all of the requisite supporting data and information, and successfully demonstrate compliance with the Act’s specific criteria. DHS will perform a comprehensive evaluation to determine your eligibility for SAFETY Act Designation or Certification. The information required in the Application is necessary for the Department to implement this critical program.

Our entire process for making available, receiving, handling, and assessing SAFETY Act Applications is completely new. We encourage and welcome feedback that will improve our procedures and enhance our ability to conduct timely and thorough evaluations of Applications.

Dr. Holly A. Dockery
Director, SAFETY Act Office
Science and Technology Division
Department of Homeland Security

PAPERWORK REDUCTION ACT

OMB Number: 1640-0001

Expiration: March 31, 2004

Public reporting burden for this collection of information is estimated to average 36 – 180 hours per response (average = 108 hours per response), including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. This is required to obtain or retain a benefit as required by Public Law 107-296 Subtitle G of Title VIII of the Homeland Security Act of 2002.

The SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies (ATTs) 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 ATTs from developing and commercializing technologies that could significantly reduce the risks or mitigate the effects of large-scale terrorist events. Without these protections, important technologies are not being deployed to counter harm resulting from a terrorist attack.

Send questions regarding any aspect of this collection of information to the Office of Science and Technology, U.S. Department of Homeland Security, 245 Murray Lane, Building 410, Washington, DC 20528 and to the Office of Management and Budget, Paperwork Reduction Project (1640-0001), Washington, D.C. 20503.

Persons are not required to respond to this collection of information unless it displays a currently valid OMB number.

TABLE OF CONTENTS

| | |
|--|----|
| I. DESCRIPTION OF SAFETY ACT AND APPLICATION PROCESS | 1 |
| A. BACKGROUND | 1 |
| 1. What is the purpose of the SAFETY Act? | 1 |
| 2. What technology is covered under the SAFETY Act? | 1 |
| 3. What protections does the SAFETY Act provide for the Sellers of ATTs? | 2 |
| 4. How do I apply? | 2 |
| 5. How does the evaluation process work? | 3 |
| 6. What does a Designation include? | 5 |
| 7. What does a Certification include? | 5 |
| B. SPECIFIC APPLICATION STEPS & TIMELINES | 6 |
| 1. How do I obtain an Application Kit? | 6 |
| 2. How do I fill out the SAFETY Act Application? | 6 |
| 3. When and how do I submit my Application? | 7 |
| 4. How long will it take for DHS to evaluate my Application? | 8 |
| II. COMPLETING SAFETY ACT APPLICATIONS – GENERAL INSTRUCTIONS | 9 |
| A. BEFORE STARTING | 9 |
| B. COMPLETING FORMS | 9 |
| C. SAVING COMPLETED FORMS | 9 |
| III. COMPLETING SAFETY ACT APPLICATIONS – ITEM-BY-ITEM INSTRUCTIONS ... | 11 |
| A. REGISTRATION | 11 |
| B. PRE-APPLICATION | 12 |
| C. DESIGNATION | 18 |
| D. CERTIFICATION | 24 |
| E. APPLICANT ACKNOWLEDGMENTS | 25 |
| IV. APPLICATION FORMS | 27 |
| A. REGISTRATION | 29 |
| B. PRE-APPLICATION | 30 |
| C. DESIGNATION | 35 |
| D. CERTIFICATION | 35 |
| E. APPLICANT ACKNOWLEDGMENTS | 35 |
| APPENDIX – PUBLIC LAW 107-296 "HOMELAND SECURITY ACT OF 2002" | 39 |

I. DESCRIPTION OF SAFETY ACT AND APPLICATION PROCESS

This SAFETY Act Application Kit facilitates the Department of Homeland Security's (DHS') implementation of Subtitle G of Title VIII of the Homeland Security Act of 2002 – the Support Anti-terrorism by Fostering Effective Technologies Act (“SAFETY Act”; see Appendix A at the back of the Kit). The Kit presents the process by which a wide range of anti-terrorism technologies (ATTs) may apply to DHS for:

1. **Designation** as a Qualified Anti-Terrorism Technology (QATT), and/or
2. **Certification** as an Approved Product for Homeland Security.

Section A of this Chapter generally documents the SAFETY Act and DHS' implementation program. The *Regulations to Support Anti-Terrorism by Fostering Effective Technologies Act*, 6 CFR Part 25 will be used to implement the SAFETY Act, once the Rule becomes final. At that time, the text of the Rule will be available at www.dhs.gov, from the U.S. Government Printing Office (www.gpoaccess.gov), or at Federal Depository Libraries around the nation. Section A also introduces the concept of a **Pre-Application, a timely method for Applicants to receive DHS feedback and guidance prior to compiling all of the detailed supporting information required as part of a full Application for Designation and Certification.**

Section B describes the specific steps that comprise the Application process, and outlines the DHS timelines associated with the evaluation of and response to an Application.

A. BACKGROUND

1. What is the purpose of the SAFETY Act?

As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted several liability protections for providers of ATTs. The SAFETY Act provides incentives for the development and deployment of ATTs 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 ATTs from developing and commercializing technologies that could significantly reduce the risks or mitigate the effects of large-scale terrorist events. The Act thus creates certain liability limitations for “claims arising out of, relating to, or resulting from an act of terrorism” where qualified ATTs have been deployed. The Act does not limit liability for harms caused by ATTs when no act of terrorism has occurred.

2. What technology is covered under the SAFETY Act?

The protections of the SAFETY Act can be extended by DHS to any qualifying product, equipment, service (including support services), device, or technology (including information technology) that is designed, developed, modified, or procured for the specific purpose of detecting, identifying, preventing, or deterring acts of terrorism, or limiting the harm that such acts might otherwise cause. This broad definition of “technology” encompasses tangible products, software, services and various forms of intellectual property.

3. What protections does the SAFETY Act provide for the Sellers of ATTs?

SAFETY Act protections available to Sellers of qualified ATTs include the following risk and litigation management provisions:

1. Exclusive jurisdiction in federal court for suits against the Sellers of “qualified anti-terrorism technologies” (Sec. 863(a)(2));
2. A limitation on the liability of Sellers of qualified ATTs 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 (Sec. 864(a)(2));
3. A prohibition on joint and several liability for non-economic damages, so that Sellers can only be liable for that percentage of non-economic damages proportionate to their responsibility for the harm (Sec. 863(b)(2));
4. A complete bar on punitive damages and prejudgment interest (Sec. 863(b)(1));
5. A reduction of plaintiffs’ recovery by amounts that plaintiffs received from “collateral sources”, such as insurance benefits or other government benefits (Sec. 863(c)); and
6. A rebuttable presumption that the Seller is entitled to the “government contractor defense” (GCD) (Sec. 863(d)).

The first five provisions are conferred to Sellers of QATTs, whereas the last provision is conferred additionally to Sellers of technologies that have received a GCD Certification. A Certification can be applied for in conjunction with or subsequent to an Application for QATT Designation, as explained below.

4. How do I apply?

Sellers of ATTs must apply formally to DHS to receive SAFETY Act protections. (Application forms are given in Chapter IV.) All of these protections, with the exception of the GCD, would be conferred upon an Applicant (i.e., Seller) if DHS determines, after a comprehensive review of the Application, that the Applicant’s ATT is a QATT. In this case, DHS will issue a Designation for the ATT to the Applicant. In order to be eligible for the GCD, DHS must conduct an additional level of review of the ATT. If the ATT successfully passes this review, DHS will issue a Certification of the Applicant’s ATT as an Approved Product for Homeland Defense. Applicants may apply for a Designation and a Certification either simultaneously or in sequence. However, obtaining a Designation is prerequisite to obtaining a Certification.

The full Designation and Certification Applications ask Applicants to assemble and document detailed supporting information and evidence, which may involve an investment of substantial time and effort. To promote overall efficiency in this process, as an alternative to submitting a complete Application, *Applicants are encouraged, but not required*, to consider first submitting a condensed **Pre-Application form**. The Pre-Application form is designed to provide several benefits to the Applicant:

- Feedback from DHS will assist the Applicant in determining what to address and emphasize in a full Application.
- Feedback from DHS may identify potential limitations and shortfalls in the existing supporting data and evidence early in the process, which might prompt additional studies or testing.
- In some cases, the Pre-Application may serve to alert DHS to potentially important technologies that may warrant further attention.

Applicants are strongly encouraged to consider first submitting a separate Pre-Application form. The contents of the Pre-Application form are included wholly within the full Designation and Certification Applications. Consequently, the Pre-Application form questions will be required to be addressed by the Applicant regardless of whether an initial separate Pre-Application form is submitted or not. The only difference is whether the Applicant wishes to take advantage of the early DHS feedback provided by the Pre-Application process in order to guide the Applicant in generating and documenting the detailed supporting data and information required by the full Application. Applicants may, without prejudice, change their Pre-Application responses when submitting the full Application, or Applicants may, upon further reflection, resubmit a Pre-Application form with updated information.

Prior to deciding whether to submit an Pre-Application, potential Applicants are strongly encouraged to read the entirety of the Application forms and accompanying Instructions to familiarize themselves with the scope and requirements of a full formal Application and to aid them in deciding whether or not to submit a Pre-Application.

5. How does the evaluation process work?

Pre-Applications are reviewed expeditiously to provide informative feedback designed to facilitate future submissions. Applications for Designation and/or Certification are evaluated with respect to the statutory criteria prescribed by the SAFETY Act.

Although a Pre-Application does not constitute an official Application, DHS will review Pre-Application submissions and, within a nominal period of 21 days, provide explicit feedback to the Applicant, including, but not necessarily limited to:

1. Summary comments on the prospective significance of the ATT to homeland security.
2. Specific comments on the responses to selected questions indicating which are either highly valued areas of interest to DHS and may warrant emphasis and scrutiny in subsequent formal Applications; or which responses might disqualify an Application for Designation or Certification unless the issue is more adequately addressed by the Applicant.
3. An overall rating of the ATT's prospects for attaining Designation and/or Certification, in terms of three levels: *promising*, *doubtful*, or *uncertain*.

DHS response to the Pre-Application is not binding on DHS with respect to other or future Applications. The three levels of DHS ratings for Pre-applications can be interpreted as follows:

Promising: This is an ATT that appears to have the potential to satisfy the criteria for a Designation (and additional conditions for a Certification).

Doubtful: This is an ATT that apparently fails or is likely to fail to satisfy the criteria for a Designation (and additional conditions for a Certification).

Uncertain: This is an ATT that, based on the information available from the Pre-Application, cannot be readily categorized as either *Promising* or *Doubtful*.

The Application forms for Designation and/or Certification ask Applicants for detailed documentation that will be reviewed and studied by DHS to evaluate technologies with respect to the statutory criteria prescribed by the SAFETY Act and implemented through the Rule. To complement the sets of data and analyses provided as part of Application submissions, DHS may consult with the Applicants or pertinent subject matter experts in order to clarify evaluation issues and to solicit specific supplementary information. An iterative process of review, dialogue, and additional requests will be used; however, contact with the Applicant is at the sole discretion of DHS. All individuals involved in the processing and evaluation of Applications, including DHS personnel, supporting administrative contractors, and government and non-government evaluators, will be bound by appropriate nondisclosure and conflict of interest agreements.

In determining whether to grant a Designation, DHS will evaluate a proposed ATT using the following criteria:

- (1) Prior U.S. Government use or demonstrated substantial utility and effectiveness.
- (2) Availability of the ATT 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 ATT.
- (4) Substantial likelihood that such ATT will not be deployed unless protections under the system of risk management provided under the SAFETY Act are extended.
- (5) Magnitude of risk exposure to the public if such ATT 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) ATT 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 DHS may consider to be relevant to the determination or to the homeland security of the U.S.

In each case, DHS will exercise discretion and judgment in interpreting and weighting these criteria, and in determining their overall significance.

In determining whether an ATT qualifies for a GCD Certification, DHS will conduct a comprehensive review of the design of the ATT and determine whether it will perform as intended, conforms to the Seller's specifications, and is safe for use as intended. The Seller will be required to provide safety and hazard analyses, and other relevant data and information regarding the ATT as determined by and requested by DHS.

6. What does a Designation include?

An Application for a Designation will culminate in either an approval or a rejection by DHS. During the review process, DHS may also reach an intermediate determination and notify the applicant that additional specified information from the Applicant is required to complete DHS' evaluation. An approval will contain an appropriate statement of Designation as a QATT, identifying the ATT and prescribing its scope of use, the term of coverage, and the liability insurance requirement. A rejection notice will describe the process the applicant must follow to obtain a detailed debriefing on the reasons for the rejection. A rejection by DHS is not subject to review, except at the discretion of DHS.

Sellers receiving a Designation must submit detailed information describing their insurance coverage as required by the terms of that Designation, and must demonstrate on an annual basis that the required insurance has been maintained. See Section 25.4 of the Rule for more details on the obligations of a Seller of a QATT.

A Designation will be valid for a prescribed period of time, varying between five to eight years, and will possibly include additional conditions explicitly imposed by DHS. Examples of potential limitations and restrictions include, but are not limited to:

- Authorized scope of applicability of the ATT, which may include the threats, targets, and other conditions of operation;
- Methods of monitoring effectiveness and responsibilities to ensure the appropriate level of effectiveness of the deployed QATT;
- Identification of critical dependencies on other technologies or capabilities in the operational environment for the QATT to be effective;
- Life cycle requirements, including but not limited to installation, training, operation, maintenance, updating, removal, or replacement the QATT;
- Critical operational specifications describing essential functions and how they will be employed in the operational setting; and
- Technical performance requirements specific to the QATT.

Sales of QATTs that are consummated during the term of the Designation will continue to benefit from SAFETY Act protections even after the expiration of the Designation. After the third anniversary of issuance of the Designation, the Seller may apply for renewal of the Designation beyond the original term. Details governing the transfer of a Designation, the extension of a Designation to licensees, and the termination of a Designation resulting from substantial modification of the QATT are described in Section 25.5 of the Rule.

7. What does a GCD Certification include?

An Application for a GCD Certification will culminate in either an approval or a rejection by DHS. During the review process, DHS may also reach an intermediate determination and notify the applicant that additional specified information from the Applicant is required to complete DHS' evaluation. An approval will contain an appropriate statement of Certification, identifying the ATT covered and prescribing any limitations or restrictions on the deployment and operation of the ATT. Additionally, the ATT will be placed on an Approved Product List for Homeland Security. A rejection notice will describe the process the applicant must follow to

obtain a detailed debriefing on the reasons for the rejection. A rejection by DHS is not subject to review, except at the discretion of DHS.

The Certification will be valid and effective for the same period of time for which the related Designation is issued, and will expire upon termination of the Designation. The Seller may apply for renewal of the Certification in connection with an Application for renewal of the related Designation. Additional details governing the transfer of Certification and the extension of Certification to licensees are covered in Section 25.7 of the Rule.

B. SPECIFIC APPLICATION STEPS & TIMELINES

There are four fundamental steps that comprise the Application process:

1. Obtain Application Kit,
2. Gather Application information and associated attachments,
3. Complete forms, and
4. Submit forms.

Applicants should note that DHS has an **Applicant Help Desk** to assist in the administrative process of obtaining an Application form, filling it out and submitting it, and to assist with the interpretation of the information requirements prescribed within the Application. Please contact 1-866-788-9318 for assistance. All of Help Desk assistance is *administrative only*; DHS employees cannot advise you on the content or substance of your Application.

1. How do I obtain an Application Kit?

The fastest way to get a copy of the SAFETY Act Application Kit, as well as to apply electronically, is via the dedicated web site at <http://www.safetyact.gov>. **The DHS web site is configured to accommodate the entire Application process, from Application form acquisition through Application submission.** Electronic Application submissions are encouraged but not required.

Application forms also are available by mail upon request sent to: Department of Homeland Security, ATTN: SAFETY Act, 245 Murray Lane, Building 410, Washington, DC 20528. Mail-in requests must be typewritten in English. Note that, as is the case for all mailings to DHS, mail requests for applications will be subjected to security checks and measures. Mail requests can be made for paper forms or for a CD format (with separate files for each section of the Application Kit). If ten business days have lapsed without a response from DHS, the Applicant should contact the DHS Applicant Help Desk to check on the status of the request.

2. How do I fill out the SAFETY Act Application?

Detailed Instructions for filling out the Application forms are provided in Chapters II and III. Again, the Applicant has the choice of electronic or paper filings; however electronic submissions are strongly encouraged in order to expedite the application process.

DHS has established protections for accepting, processing, evaluating, and reporting on technical, business and insurance data and information that are proprietary or sensitive. All Applications, whether paper or electronic, will be subject to these stringent safeguards. There is

no need for Applicants to be unduly apprehensive and to constrain the scope of the material offered to DHS as part of any Application. Limiting information in your Application may delay evaluation. Neither is there any need to identify and distinguish any specific data elements or segments of materials as being proprietary or sensitive – as everything in the Application will be accorded the same secure handling and treated as if it were proprietary.

Additionally, DHS has established protocols to ensure that the Department will utilize all appropriate exemptions from the Freedom Of Information Act.

Under no circumstances is U.S. Government classified information to be entered in or submitted as part of any Application. If the Applicant believes that classified materials are essential to answering an Application question or fully documenting the subject ATT's design, capabilities and demonstrated performance, a completely *unclassified* overview description of the information in question should be inserted as an attachment to the Application. If DHS evaluators subsequently concur that classified inputs are needed to support comprehensive assessments, DHS will identify specific classified information requirements and request that the Applicant forward the same to DHS as part of the extended Application review process. The precise means for accommodating the transmission of the classified inputs from the Applicant to DHS will be detailed in the formal request notice that DHS will send to the Applicant. DHS has established appropriate protocols for accepting, processing, evaluating, and reporting on classified material.

3. When and how do I submit my Application?

Application forms may be submitted to DHS either electronically via the dedicated web site <http://www.safetyact.gov>, or by mail sent to: Department of Homeland Security, ATTN: SAFETY Act, Washington, DC 20528. The web site and the electronic submission procedures can be accessed by Internet Explorer, Netscape, and other common browsers. Any problems or difficulties encountered should be reported to the Help Desk. To be accepted electronically, all attachments must be written in English and must be readable in one of the following formats: .PDF, .RTF, .CSV, .DOC, or .XLS.

Mail-in Applications, either paper or CD-ROM (with attachments adhering to .PDF, .RTF, .CSV, .DOC, or .XLS formats) must be typewritten in English. Again note that, as is the case for all mailings to DHS, mailed submissions will be subjected to security checks and measures. No hand deliveries, facsimile (fax) transmissions, or e-mail submissions will be accepted. Applicants can verify that their Application has been received by DHS, by checking the DHS web site or by contacting the DHS Applicant Help Desk.

All paper Applications will be converted to electronic format by DHS to facilitate subsequent processing, evaluation, tracking, and archiving. A paper copy of the reformatted Application will be forwarded by DHS to the Applicant in order to obtain formal verification that the reformatted Application is complete and accurate. If the Applicant has provided an e-mail address and if e-mail correspondence has been explicitly authorized, an electronic copy will be transmitted in lieu of a paper copy. The Applicant must review the information on the reformatted Application and formally transmit verification or corrections to DHS before the Application will be further processed. Instructions for how to respond with verification or

corrections will be supplied with the reformatted Application. The initial 30-day review for completeness will begin once DHS officially receives verification from the Applicant of correctness of the Application.

The first part of any initial Application for an ATT is the Registration by the Applicant, which must be submitted separately. Prompted by the Registration, DHS will assign to the Applicant a unique Applicant ID. This code is to be utilized by the Applicant in all subsequent Applications, possibly encompassing multiple ATTs.

As a precaution and to support future submissions and correspondences with DHS, the Applicant is encouraged to make and retain an electronic or paper copy of any submission.

4. How long will it take for DHS to evaluate my Application?

DHS will review Pre-Application submissions within a nominal period of 21 days.

DHS will review each Application for completeness and respond to the Applicant within 30 days with either a request for more information (for incomplete applications) or notification that the Application is complete and will be submitted for evaluation. Here and throughout the remainder of this subsection, “Application” refers to either an Application for Designation or an Application for Certification.

During the evaluation process, DHS may request that the Seller provide additional information, may consult with the Applicant and other government agencies or private entities, and may perform various studies. Within 90 days after receipt of a complete Application, the Assistant Secretary for Plans, Programs, and Budget of the Department of Homeland Security Directorate of Science and Technology (“the Assistant Secretary”) will recommend to the DHS Under Secretary for Science and Technology (“the Under Secretary”) whether the ATT should be approved or rejected for a Designation / Certification. The Assistant Secretary may also report to the Under Secretary that the ATT could potentially receive a Designation / Certification but that more information is needed to complete the evaluation. The Assistant Secretary may, without cause or explanation, extend the review period beyond 90 days upon notice to the Applicant.

Within 30 days after receiving a recommendation from the Assistant Secretary, the Under Secretary will approve or deny the Application, or notify the Seller that the ATT is potentially eligible for a Designation / Certification, but that more information is required to make a decision. The Under Secretary may, without cause or explanation, extend the review period beyond 30 days upon notice to the Applicant. The Under Secretary’s decision to accept or reject the Application is final. It is not subject to review, except at the Under Secretary’s discretion. Instructions for communications with DHS after your Application is either accepted or rejected will be provided at the time you are informed of the decision.

II. COMPLETING SAFETY ACT APPLICATIONS – GENERAL INSTRUCTIONS

A. BEFORE STARTING

Before initiating the filling out of any Application form, the Applicant is advised to first view the relevant portions of the form, determine in advance which entries will be checked and entered, and assemble all the requisite supporting material – in paper for a paper submission, and in an appropriate electronic form for electronic submission. Additional suggestions supporting electronic submission appear on the web site.

B. COMPLETING FORMS

The following requirements apply to both electronic and paper submissions:

1. Applications must be typed in English.
2. Use Times New Roman font (or comparable easy-to-read font), 12-point minimum.
3. Use normal default line spacing, i.e., a minimum of single space.
4. Adhere to the response and page limits stipulated in Chapter III.
5. Unless otherwise indicated, all requested data fields are mandatory and must be filled in (“N/A” for “not appropriate” or “not available” may be inserted).
6. Define any abbreviations that may be unfamiliar to readers.
7. Use either exclusively English units or exclusively metric / System International units.
8. All monetary values should be expressed in terms of then-year U.S. Dollars.
9. As appropriate and specifically identified, amplifying information should be included as attachments:
 - a. Explicitly link each entry in all attachments to its corresponding Section and Item from the Application form.
 - b. For any multi-page attachments in response to a single Application form Item:
 - i. Use one-inch top, bottom, left, and right margins.
 - ii. Number pages sequentially.

Additional requirements that apply to paper-based filings include:

- Use 21.6 x 27.9 cm (8½ x 11 in) paper.
- For the attached material only, print on both sides of the paper.
- If the originals of figures and drawings are in color but black and white copies are being submitted, ensure that the plots are still understandable; lines are identifiable and differentiable, etc.

C. SAVING COMPLETED FORMS

As a precaution and to facilitate future submissions and dialogue with DHS, the Applicant is encouraged to make and retain an electronic or paper copy of any submission.

III. COMPLETING SAFETY ACT APPLICATIONS – ITEM-BY-ITEM INSTRUCTIONS

These Instructions are divided into the five sections of the Application form:

- A. REGISTRATION
- B. PRE-APPLICATION
- C. DESIGNATION
- D. CERTIFICATION
- E. APPLICANT ACKNOWLEDGMENTS.

Here are four important notes to remember:

1. The first step for any Applicant is to fill out and submit a Registration.
2. Upon Registration, DHS will assign a unique Applicant ID to the Applicant, which the Applicant is required to enter in all subsequent Applications.
3. Updated Registrations are required whenever any of the information requested on the Registration form changes.
4. The first step for any Application is to complete Item 1 of the Pre-Application form.

A. REGISTRATION

Item 1. Check exactly one of the boxes in the first line. If this is the initial registration by the Applicant, check the first box and proceed to Items 2 and 3. If the Applicant has been registered previously but some of the relevant information on the Registration form has changed and requires revision, check the second box, enter the Applicant ID previously supplied by DHS, and proceed to enter all of the new or revised information into the appropriate lines in Items 2 and 3. The remainder of the lines, which involve no changes, should be left blank. It is important to update the Registration whenever any of the basic information called for in Section A changes.

Item 2. Item a and Items c – e are mandatory (except for “Line 2” in the Address); the remaining lines may be left blank. If the company has a nine-digit DUNS number, enter it at Item b. If the company does not have a DUNS number, it is unnecessary to obtain one. The Application will not be rejected due to lack of a DUNS number. NAICS Codes can be found in the official 2002 US NAICS Manual *North American Industry Classification System – United States, 2002* (available from the National Technical Information Service, (800) 553-6847 or (703) 605-6000) or directly from <http://www.census.gov/>. Include area codes and non-U.S. country codes with all telephone numbers.

Item 3. This information pertains to the initial principal Point Of Contact (POC). It is understood that, in support of the comprehensive DHS evaluation process, additional lines of communication may need to be established with other Seller representatives. Note that the items requested here ask only for office or business contact information, i.e., no personal or home contact information is being sought. Lines a – c are mandatory (except for “Line 2” in the Address); and the remaining lines may be left blank. Enter Name as Last, First, Middle Initial. Include area codes and non-U.S. country codes with all telephone numbers. If an e-mail address is provided in Line e, it is mandatory to check exactly one of the two boxes in Line f. Check the “Yes” box only if subsequent e-mail exchanges between DHS and Seller representatives are authorized to facilitate administrative communications and to reduce processing timelines.

Note: Once the Registration has been submitted and the acknowledgment and the Applicant ID from DHS have been received (this should be no more a few minutes for electronic submissions), the Applicant may proceed with the Application. All Applications must begin with Item 1 in Section B. Depending on the type of Application that is specified, the Applicant will be directed to particular portions of the Application form. A unique Application Number will be generated by DHS and reported to the Applicant. Past versions of any Application can be retrieved readily from the dedicated web site, and easily modified and re-submitted.

B. PRE-APPLICATION

Important: Chapter IV Section B, the “Pre-Application Form” must be filled out if you are submitting a Pre-Application only, or if you are applying for Designation only, or if you are applying simultaneously for Designation and Certification. Carefully read and adhere to Section B Item 1.b in the Instructions below.

This section is partitioned into groupings of Items associated first with a description and characterization of the subject ATT, and then with the specific SAFETY Act Evaluation Criteria prescribed within the Act and the Rule.

Item 1.a. Enter the Applicant ID (provided by DHS upon submission of the Registration, i.e., Section A). If all of the information from the last submitted Registration form remains valid, check the “Yes” box. If an update is required, stop filling out Section B. Instead, complete and re-submit Section A again, reflecting the changes, and await DHS acknowledgement before proceeding anew with Section B.

Item 1.b. Check exactly one box. Indicate which type of Application is being submitted: Pre-Application, Designation only, simultaneous Designation plus Certification, or Certification only (given previous Designation). If any one of the first three boxes is checked, complete the remainder of Section B and add attachments as indicated in the corresponding Instructions. If the “Designation” box is checked, also add the attachments prescribed in Section C below. If the “Designation + Certification” box is checked, add the attachments prescribed in Sections C and D below. If the last “Certification only” box is checked, provide the associated DHS Designation Number, and check each of the next two boxes if the particular indicated circumstances for the ATT have remained constant since Designation. The Application for Certification will not be processed unless these two boxes are checked or an appropriate explanatory narrative (no more than 5 sentences) is attached. All Applications except the informal Pre-Application require Section E, the Applicant Acknowledgments, to be completed. For electronic submissions, note that previous Applications can be retrieved, edited, and resubmitted.

Item 1.c. REQUIRED: As an attachment, provide a brief **completely non-proprietary** overview description of the ATT (no more than 20 lines of text), suitable for screening potential evaluators for conflict of interest. Identify explicitly any other known similar technologies or any other known substantially equivalent technologies – in concept phase, in development, available but not deployed, operationally deployed, DHS Designated / Certified, or other. Identify explicitly any corporate parent, partners, and related business affiliations – both for the company as a whole and for portions dedicated to the ATT.

Note: Items 2 – 5.a identify and characterize fundamental aspects of the ATT – supporting sorting into particular evaluation groupings (including the assignment of specific evaluators) and exploring whether the ATT warrants expedited processing as required by the Act and the Rule (Items 2.c, 2.d and 5.a). The links to similar technologies and any relevant historical usage identify specific sources of information that can facilitate the DHS evaluation process.

Item 2a. Enter the ATT name. Also, as appropriate, enter the ATT make and model descriptions to completely distinguish and identify the subject ATT. Otherwise, the make and/or model lines may be left blank.

Item 2.b. REQUIRED: Check “Yes” and, as an attachment, **provide a brief executive summary** (no more than one page) of the ATT describing: nature and characteristics of the technology, relevant threat scenarios (typical as well as a plausible high-loss scenario), demonstrated performance capabilities and limitations, potential safety issues, outline of business plan, and outline of insurance plan. Use the content of the remaining Items in Section B to help fashion this executive summary.

Item 2.c. Check exactly one box. If it is known that the subject ATT is substantially equivalent to another ATT that already has received DHS Designation / Certification, check the “Yes” box, and, if available, provide the corresponding DHS Designation / Certification number (to permit expediting the processing for and evaluation of the subject ATT). Note that 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.

Item 2.d. Check exactly one box. If the ATT is being procured by a federal agency, either at present or anticipated in the near future, check “Yes” and supply the requested information. This will support expediting the processing for and evaluation of the subject ATT. Lines i – iv are mandatory (except “Line 2” in the Address); the remaining lines may be left blank. Enter Name as Last, First, Middle Initial. Include area codes and non-U.S. country codes with all telephone numbers.

Items 3.a & 3.b. Consider the following technological elements:

- | | | |
|--------------------------|--|------------------------|
| 1. Hardware / equipment | 2. Computer software | 3. Bio-tech components |
| 4. Personnel / operators | 5. Skilled services | 6. Mobile platforms |
| 7. Logistics / supplies | 8. Embedded intellectual property (including analyses) | |
| 9. Networking | 10. Other | 11. None |

Using the indicated enumeration to represent these elements, select and enter the most significant technological elements (at least one and up to three distinct entries) that comprise the ATT itself (e.g., “1, 2, 6”). Similarly, select and enter the most significant technological elements (up to three distinct entries; if “None” is appropriate enter “11” in the first fill-in box) that are external but essential to the ATT. Consider all interfaces with the ATT, including own company, other companies, public utilities, government, etc.

Item 4.a. Check exactly one box.

Item 4.b. Check all that apply. At least one box must be checked.

Item 4.c. Check all that apply, unless the specific threat information would be classified. In that case, see the discussion in Chapter I, Section B.2 that describes how classified information should be handled.

Item 4.d. From the list of enumerated potential terrorist targets provided below, choose from one to three that best represent the primary targets defended by the ATT (e.g., “P2, I5, V1”). Likewise, choose up to three distinct secondary targets; if “none” is appropriate enter “N” in the first fill-in box. For target type B7, “Non-profit” should be interpreted as “Non-Government, Non-Profit” organizations such as universities, science and technology centers, charities, etc.

People

P1. Crowds / special events systems)

P2. General population dispersed nationwide

P3. General population in localized area

P4. Prominent individuals

Buildings / Facilities

B1. Large urban areas

B2. Nuclear power plants

B3. Airports

B4. Seaports / river & lake ports

B.5 Rail / subway terminals

B6. Warehouses, distribution centers & freight consolidation points

B7. Commercial & non-profit buildings /facilities

B8. Government buildings /facilities

B9. Residences

B10. National monuments / icons

O1. Other

Infrastructure Systems / Capabilities

I1. IT (databases, networks, computer &control systems)

I2. Telecommunications

I3. Defense industrial base

I4. Banking / finance

I5. Transportation (corridors, bridges, tunnels, locks)

I6. Energy (production, storage, distribution)

I7. Chemical / hazardous materials industry

I8. Agriculture / food

I9. Water (production, storage, distribution)

I10. Emergency services

I11. Public health

I12. Border check points (air, sea, road, rail)

I13. Postal/shipping

Vehicles

V1. Aircraft

V2. Ships / boats

V3. Trains

V4. Automobiles / Trucks

Item 5.a. Check all that apply; at least one box must be checked. Here “Non-profit” should be interpreted identically as in the preceding Item 4.d. The fifth category encompasses U.S. carriers at international destinations and along international travel routes.

Note: Item 5.b pertains directly to Evaluation Criterion 1:

- *Prior U.S. Government use or demonstrated substantial utility and effectiveness.*

Item 5.b. Check all that apply. The choices and their interpretations are identical to that described for the preceding Item 5.a.

Note: Item 6 pertains directly to Evaluation Criterion 2:

- *Availability of the ATT for immediate deployment in public and private settings.*

Item 6.a. Consider the following characterizations of the state of a technology's maturity:

1. Employed in military or counter-terrorism missions,
2. Production items available and mature concept of operations established,
3. Production items available,
4. Licensed producer exists,
5. Developmental units available and have passed operational tests,
6. Prototype units available,
7. Manufacturing specifications established, and
8. Conceptual phase.

Select the best characterization of the subject ATT and enter the associated number from above (e.g., "6").

Item 6.b. Check exactly one box. If the third box is checked, enter a projected availability date (month and year).

Item 6.c. Check exactly one box under "Entire", and Check exactly one box under "Limited". Assume that a go-ahead decision has been reached, that all requisite authorizations have been obtained, and that the only issue is how quickly the ATT can be produced, delivered, and deployed.

Note: Items 7 - 10 pertain directly to the inextricably related Evaluation Criteria 3 and 4:

- *Existence of extraordinarily large or extraordinarily unquantifiable potential third party liability risk exposure to the Seller or other provider of such ATT, and*
- *Substantial likelihood that such ATT will not be deployed unless protections under the system of risk management provided under the SAFETY Act are extended.*

Item 7.a. If there is no current insurance coverage, check all of the boxes that apply (although logically not both of the first two boxes can be checked). Otherwise, enter all available values and information, using then-year U.S. Dollars for all monetary values. Blanks are permissible. Add attachments as needed to provide values, definitions, and other amplifying information. Limit each individual response (to a specific information query) to no more than two lines of text.

Item 7.b. If there are no additional insurance quotes, check either or both boxes, as appropriate. Otherwise, enter all available values and information, using then-year U.S. Dollars for all monetary values. Blanks are permissible. Add attachments as needed to provide values, definitions, and other amplifying information. Limit each individual response (to a specific information query) to no more than two lines of text.

Item 8.a. If no estimates are available, check the box and proceed to Item 9. Otherwise, proceed to Item 8.b.

Item 8.b. Check all boxes that apply. Blanks are permissible. For any checked box, also add any available dollar estimates or otherwise leave blank, considering separately typical and plausible high-loss scenarios.

Item 9.a. If no estimates are available, check the box and proceed to Item 10. Otherwise, proceed to Items 9.b and 9.c.

Items 9.b & 9.c. In each case, check all that apply. Blanks are permissible. If “Other” is checked, attach a short explanatory text (no more than three lines).

Item 10.a. If no business plan has been developed, check the box and proceed to Item 11. Otherwise, proceed to Items 10.b - 10.e.

Items 10.b & 10.c. If available, for each case estimate the size of the market (expressed in terms of millions of then-year U.S. Dollars) and the percentage share (integer between 0% and 100% inclusive) attributable to the Applicant.

Items 10.d & 10.e. Both Items refer to the timetables provided previously in the responses to Item 6.c. For each Item, check exactly one box. Item 10.d asks whether the business plan is consistent with the timetables presented in the response to Item 6.c. Item 10.e asks for the status of the expertise and resources required to execute those timetables, e.g., already in hand, or planning is underway, or no plans have been initiated.

Note: Items 11 - 13 pertain directly to Evaluation Criterion 5:

- *Magnitude of risk exposure to the public if such ATT is not deployed.*

Items 11.a & 11.b. For each Item, check “None” or all that apply. Here “risk exposure” includes considerations of both likelihood of attack and the impact of attacks.

Item 12.a. For each of the six categories of harm provided below, consider the typical-case terrorist act scenario articulated in response to Item 2.b, and in the top row enter the best estimate of harm from the tabled choices below (e.g., “F3.”). If no estimate is available or appropriate, enter “N”. There should be six entries, one per category of harm, and at least one should be a non-“N” other than “F0”, “I0”, “E0”, “P0”, “M0”, or “S0”. Proceed similarly for the plausible high-loss terrorist act scenario articulated in response to Item 2.b, and complete the second row.

Fatalities:

Chose from: F0. None
F1. 1-10
F2. 10-100
F3. 100 – 1,000
F4. 1,000 – 10,000
F5. 10,000 – 100,000
F6. 100,000 – 1,000,000
F7. More than 1,000,000

Injuries:

Chose from: I0. None
I1. 1-10
I2. 10-100
I3. 100 – 1,000
I4. 1,000 – 10,000
I5. 10,000 – 100,000
I6. 100,000 – 1,000,000
I7. More than 1,000,000

Economic Losses (Then-Year U.S. \$):

Chose from: E0. None
E1. \$0 to \$100 million
E2. \$100 million - \$10 billion
E3. \$10 billion - \$1 trillion
E4. Over \$1 trillion

| Physical Damage | Mass Disruption (attacks on infrastructure or general fear) | Symbolic Damage (monuments, icons, cultural treasures or environment) |
|----------------------------------|--|--|
| Chose from: P0: None | Chose from: M0: None | Choose from: S0: None |
| P1. Car/Truck | M1. Major organization | S1. Known Locally |
| P2. Airplane/Ship | M2. Metropolitan area | S2. Known by major elite group |
| P3. Building | M3. State or region | S3. Known regionally |
| P4. Complex of structures | M4. All U.S. | S4. Known nationally |
| P5. Large neighborhood | M5. Global | S5. Known internationally |
| P6. City | | |
| P7. Agriculture & Infrastructure | | |
| P8. Multi-state region | | |

Item 12.b. For the same events entered in Item 12.a, indicate the estimated percentage reductions expressed in terms of integers between 0% and 100% (where 100% corresponds to completely reducing the potential harm).

Item 13. Check all that apply. At least one box must be checked.

Note: Items 14 - 20 pertain directly to the inextricably related Evaluation Criteria 6 and 7:

- *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.*
- *ATT that would be effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat or respond to such acts.*

Item 14. Check either “None” or all of the following that apply. There must be at least one checked box. Going from left to right, the non-“None” choices of analytical measures respectively denote broad performance statements (“Objectives”), lists of functional performance steps (“Functions”), measures of performance (“Metrics”), and measures augmented by associated quantitative or qualitative performance thresholds (“Metrics & specified criteria”).

Item 15. Check either “None” or all of the following that apply. There must be at least one checked box. Here “Red team ‘attacks’” denotes planned simulated attacks on the ATT that are unknown to the operators and users of the ATT.

Items 16.a – 16.c. For each row, assume a plausible high-loss event for harm potentially induced by the ATT itself. Then for each of the six damage categories, enter the estimate of harm using the codes provided above for Item 12.a. If no estimate is available or appropriate, enter “N”. If there is no expectation of any possible harm attributable to the ATT, all of the entries would be comprised of some combination of “N”, “F0”, “I0”, “E0”, “P0”, “M0”, and “S0”.

Items 17.a. Check either “None”, or one or both of the following that apply. There must be at least one checked box. If “None” is checked, skip the remaining items and proceed directly to Item 18. If “None” is not checked, complete Items 17.b – 17.e.

Items 17.b –17.e. Check either “None”, or all of the following that apply. There must be at least one checked box.

Items 18.a – 18.h. Consider the following hierarchy of potential types of evidence:

7. Operational deployment as an ATT,
6. Other operational deployment,
5. Independent operational tests,
4. Independent tests,
3. Company tests,
2. Independent studies and analyses,
1. Company studies and analyses, and
0. None

For each letter, respond by entering the one or two highest levels of supporting evidence (where “7” is the highest attainable) that apply, with the lower number entered first, e.g., “1 4”. If there is only one type of available evidence, enter “0” in the first blank (to the left) and enter the other positive number in the rightmost blank. If there is no available evidence, enter “0 0”. For Items 18.c – 18.h, enter “N/A N/A” if the specified aspect of operational performance is inapplicable to the ATT.

Items 19.a – 19.f. For each Item, use the same hierarchy of potential types of evidence as in Item 18, except now exclude Categories 1 and 2 from the potential responses. Likewise, fill in each pair of blanks according to the exact procedures prescribed for Item 18. Note that the threat designations are shorthand representations of the more complete descriptions listed in Item 4.a. of the Pre-Application form.

Items 20.a – 20.d. Proceed as for Items 19.a – 19.f. Note that the asset designations are the target groupings listed in the Instructions for Item 4.d above.

Item 20.e. If additional classes of assets beyond those listed in Items 20.a – 20.d are required, fill in Item 20.e, check “Yes”, and add a brief attachment (no more than two lines of text per additional class).

C. DESIGNATION

Important: Responses are required to Items 1 – 14 in this Section C if you are applying for Designation only, or if you are applying simultaneously for Designation and Certification. In either case, you must also complete the “Pre-Application Form” in Chapter IV, Section B.

For Items 1 - 10 below, a response will be provided as a single attachment. Each Item's response should consist of a short overview narrative followed by a summary-level compilation of appropriate supporting documentation comprised of dedicated sets of text and/or citations to and synopses of available complete reports. All supporting documents and reports cited in the application attachment should also be appended to your application. If documents or reports cited in the application are not included at the time of submission or not otherwise readily available, DHS may deem the application incomplete. Note that responses appearing elsewhere in this Application or in other attachments should be cited only (e.g., "See Section X Item Y.Z") and not repeated verbatim. Instructions for Items 11 - 14 follow separately below. While certain Items below relate explicitly to specific identified criteria, a response to any Item may be used to evaluate any of the evaluation criteria.

1. Provide a **brief** description of the technology – including the following items:
 - a. Mission statement;
 - b. Deployment history;
 - c. Key subsystems;
 - d. Functionality;
 - e. Underlying scientific principles and unique technology attributes distinguishing the ATT from alternatives that could provide similar anti-terrorism capabilities; and
 - f. Index of related intellectual property dispositions, i.e., patents, trademarks, copyrights, etc., either in the U.S. or internationally.
2. Describe the critical end-to-end steps / events that comprise the operating profile for the ATT, including all key subsystems, interfaces, and complementary systems:
 - a. Under likely and extreme operating conditions, while countering specific types of **actual** terrorist attacks.
 - b. Under likely and extreme operating conditions, in a readiness or standby mode awaiting a **potential** terrorist attack.
 - c. Against plausible countermeasure tactics.
 - d. Summarize the key operating profile differences between Items 3.a – 3.c.
3. Describe in detail the envisioned threat scenarios that the ATT is intended to counter. Focus on both typical and plausible high-loss threat scenarios.
4. Describe the complete steps and supporting activities required by the buyers and users of the technology to deploy, implement, and operate it as an ATT. Include projected timetables, manpower and training requirements, etc. *(Relate explicitly to Evaluation Criterion 2 and Section B Item 6.)*
5. Describe and document the studies and reports supporting your assessments of potential third party liability risks and other potential liability issues associated with the ATT. Focus on both typical and plausible high-loss scenarios. *(Relate explicitly to Evaluation Criterion 3 and Section B Items 7 - 9. Include considerations of the impact of Quality Control / Quality Assurance programs.)*
6. Describe and document the studies and reports supporting assessments of the likelihood that your technology would **not** be deployed as an ATT without the benefits of the SAFETY Act. Include the possible effects of the cost of insurance on the price of the product, and the possible consequences thereof on development, marketing, manufacture, qualification, sale, transportation, use, operation, support, and removal of the ATT. *(Relate explicitly to Evaluation Criterion 4 and to Section B Items 7 – 10. Include considerations of the impact of Quality Control / Quality Assurance programs.)*
7. Describe and document the studies and reports supporting assessments of the magnitude of risk exposure to the public, with and without the deployment of the ATT. Focus on both typical and plausible high-loss threat scenarios. *(Relate explicitly to Evaluation Criterion 5 and Section B Items 11 - 13.)*

8. Describe and document measures for evaluating the expected operational performance of the technology as an ATT, and the means for monitoring and assessing these measures post-deployment. (Relate explicitly to Evaluation Criteria 6 and 7 and to Section B Items 14 and 15.)
9. Describe and document the scientific studies or other types of corroborative evidence that demonstrate that the technology has substantial utility and effectiveness as an ATT, or that otherwise would support an assessment of the capability of the technology to substantially reduce risks of harm. (Relate explicitly to Evaluation Criteria 6 and 7 and to Section B Items 16 - 20.)
10. Document all known or suspected current hazards and safety issues associated with the ATT – covering the entire life cycle of development, marketing, manufacture, qualification, sale, transportation, use, operation, support, and removal. Summarize all related historical hazard concerns and safety incidents that were encountered in development, testing, and operational use, as well as all remedial actions taken.

The remaining Items in this section request detailed insurance and financial information, in support of Section C Items 5 and 6. The provided responses will permit DHS evaluators to perform the independent assessments of maximum allowable liability insurance prescribed within the Act and the Rule. Document all responses as attachments – no more than 10 pages for Item 11, and sufficient pages for Items 12 – 14 to present the requested matrices. Note that all monetary values should be expressed in terms of then-year U.S. Dollars.

11. Provide any risk management plan and risk analyses related to the ATT for the past three years. Enumerate potential liabilities relevant to the ATT and their probability and magnitude. Distinguish between risks related to a terrorist act and those unrelated. Distinguish among potential liabilities for economic damages, punitive damages and other non-economic damages. Focus on both typical and plausible high-loss scenarios.
 - a. For the past three years, with respect to liability insurance purchased for the business as a whole and for the ATT specifically, or for other technologies, if applicable, provide the following:
 - i. Name of insurer;
 - ii. Types of coverage;
 - iii. Annual premium and estimate:
 1. The amount of (or percentage of premium directly attributable to) protection against liability arising out of a terrorist act, and
 2. The amount of (or percentage of premium directly attributable to) protection associated with the ATT in an aggregate liability policy;
 - iv. Amounts of coverage;
 - v. Relevant terms of coverage;
 - vi. Dollar limits for products and completed operations;

- vii. **Dollar limits per occurrence and annually, including applicable sub-limits;**
 - viii. **Any limitations on number of occurrences;**
 - ix. **Deductibles and/or self-insured retentions;**
 - x. **Exclusions or other restrictions or limitations on coverage;**
 - xi. **Whether the coverage includes contractors, subcontractors, suppliers, vendors, customers, or customers' contractors, subcontractors, suppliers, or vendors.**
- b. **If applicant self-insures or plans to self-insure, submit all information described in 48 CFR 28.308(a)(1)-(a)(10).**
 - c. **Describe any unsuccessful attempts to purchase insurance coverage that would be applicable to third-party claims against the ATT.**
 - d. **Provide any benchmarking information used to arrive at applicant's level of liability insurance coverage or coverage specific to the ATT.**
 - e. **Provide information on the amount of liability insurance offered on the world market.**
 - f. **Provide data and history on mass casualty losses in situations comparable to those terrorist acts that the ATT is intended to counter.**
 - g. **Provide a point of contact (including phone number) that is authorized to discuss the Seller's insurance information.**

12. Financial Information. In an attachment formatted like Table 12 below (a read/write downloadable format provided online at <http://www.safetyact.gov>), follow the subsequent directions. As appropriate, add more columns (years) or rows (cost/revenue/depreciation/etc. elements) in Table 12 (and for all subsequent tables), providing the complete table on an additional page(s). When using units, carefully define how "units" are measured with a footnote in the Table. Place all required footnotes at the outside base of the Table.

- a. In Table 12 provide details of the existing ATT income statement (selling price, cost, and annual production volume) as currently marketed – on either a total cost basis or a per unit cost basis (cross-reference with the information in Section C Item 11 above). The indicated costs must be the costs that are used to measure and record any inventory of this ATT, i.e., exclude allocated central overhead costs such as R&D or headquarters staff that are not dependent on the product or service in question. Sales of this ATT may already be for "commercial" use in addition to government or military sales.
- b. Indicate, using footnotes, when standard costs are being utilized and identify the variances from standard when used as a component of "Total technology cost" in the "other" cost category if they are not spread back to material, labor and overhead.
- c. If the answer to Q1 in Table 12 is "No" for any year, explain the difference between the costs included in inventory and the costs noted above in a footnote.
- d. If the answer to Q2 in Table 12 is "Yes" for any year, explain how the standards were adjusted for variances in a footnote.

- e. Indicate the cost and revenue data provided in Table 12 that auditors could not trace in your records and explain how it was estimated in appropriate footnotes.
- f. In a separate discussion associated with Table 12, not a footnote, identify the top five customers for this technology by sales dollars and indicate, if the selling price varies by customer, what the current selling price per unit of technology is by customer or explain why this cannot be provided.

Table 12. Technology Cost Data: Historical Costs (Then-Year U.S. Dollars)

| Cost and Revenue data for technology as <u>currently marketed</u> | | | |
|--|--|---|---|
| | Indicate <input type="checkbox"/> total costs or <input type="checkbox"/> unit costs | | |
| | <u>2003E</u> | <u>2002</u> | <u>2001</u> |
| <u>Sales revenues – net</u> | \$ | | |
| <u>Technology Costs:</u> | | | |
| Direct Materials (Raw Material and Purchased Parts) | \$ | | |
| Direct Labor | \$ | | |
| Overhead (Describe cost components included)) | \$ | | |
| Other (describe cost components included) | \$ | | |
| <u>Total technology costs</u> | \$ | | |
| Gross Profit (Sales Revenue – Total Tech. Cost) | \$ | | |
| Please break out the total technology costs above into variable and fixed costs: | | | |
| Variable <u>total technology costs</u> if known | \$ | | |
| Fixed <u>total technology costs</u> if known | \$ | | |
| Units of Production | | | |
| Units of Sales | | | |
| Q1. Is inventory cost made up of the costs above? Yes or No | <input type="checkbox"/> Y <input type="checkbox"/> N | <input type="checkbox"/> Y <input type="checkbox"/> N | <input type="checkbox"/> Y <input type="checkbox"/> N |
| Q2. Standard costs used? Yes or No | <input type="checkbox"/> Y <input type="checkbox"/> N | <input type="checkbox"/> Y <input type="checkbox"/> N | <input type="checkbox"/> Y <input type="checkbox"/> N |
| Q3. Indicate the % of commercial sales each year, if any. | | | |

13. Prospective Data. In an attachment formatted like Tables 13-1 through 13-2 below (a read/write downloadable format provided online <http://www.safetyact.gov>), provide prospective data for the candidate ATT, on the same basis and comparable to the data in Table 12. If forecasts are available for different volumes of sales at different market prices, use column 2004ML to represent the most likely forecast, 2004H to be the highest volume (lowest price) forecast, and 2004L to be the lowest volume (highest price) forecast – all assuming that the ATT is approved under the SAFETY Act. Cross-reference with the information in Section C Item 11. If there is a risk premium for possible lawsuits in conjunction with the sale of this product built

in to its price in Table 13-1, indicate that value. If estimates exist for years beyond 2006, please add columns to Table 13-1 to show those estimates.

Line up the revenue and costs between the latest year in Table 12 and the first year in Table 13-1, and explain any variance in an attachment formatted like Table 13-2. With the exception of the risk premium associated with the new application of this ATT, the revenues, costs and profits of the ATT are expected to change on the basis of the traditional cost-volume-profit framework. To the extent that this traditional framework does not apply, explain in a footnote associated with Table 13-2. Describe the nature and cause of any changes in the costs or revenues between Tables 12 and Table 13-1 that are **not** related to pricing of additional risk (if any). These changes should be associated with the expanded application of this ATT to commercial customers (or to additional commercial customers if some commercial customers already exist).

Table 13-1. Technology Cost Data: Prospective Cost (Then-Year U.S. Dollars)

| Cost and Revenue data for technology if certified as anti-terrorism device | | | | | |
|--|------------------------------------|--------------|--------------|-------------|-------------|
| | Indicate total costs or unit costs | | | | |
| | <u>2004ML</u> | <u>2004H</u> | <u>2004L</u> | <u>2005</u> | <u>2006</u> |
| <i>Sales revenues – net</i> | | | | | |
| <i>Technology Costs:</i> | \$ | | | | |
| Direct Materials (Raw Material and Purchased Parts) | \$ | | | | |
| Direct Labor | \$ | | | | |
| Overhead (Describe cost components included) | \$ | | | | |
| Other (describe cost components included) | \$ | | | | |
| <i>Total technology costs</i> | \$ | | | | |
| Gross Profit (Sales Revenue – Total Tech. Cost) | \$ | | | | |
| Please break out the total technology costs above into variable and fixed costs: | | | | | |
| Variable <i>total technology costs</i> if known | \$ | | | | |
| Fixed <i>total technology costs</i> if known | \$ | | | | |
| Units of Production | | | | | |
| Units of Sales | | | | | |

Table 13-2. Changes in Revenues and Costs (Then-Year U.S. Dollars)

| Component | Explanation of Variance -Table 12 vs. Table 13-1 | | |
|-----------------|--|--------|-----------------------|
| | 2003E | 2004ML | Explanation of Change |
| Revenue | \$ | | |
| <u>Cost</u> | | | |
| Direct Material | \$ | | |
| Direct Labor | \$ | | |
| Overhead | \$ | | |
| Other | \$ | | |

14. Product Related Spending. In an attachment (a read/write downloadable format is provided online at <http://www.safetyact.gov>), provide the capital and project-related spending (e.g. tooling, equipment, engineering, etc) required to deploy the anti-terrorism technology. Include spending already paid as well as estimates for future expenses. Break up the expense, in then-year US Dollars, into the years in which it was paid.

D. CERTIFICATION

Important: Responses are required to Items 1 – 3 in this Section D if you are applying simultaneously for Designation and Certification, or if you are applying for Certification only. In the former case, you must also complete the “Pre-Application Form” in Chapter IV, Section B, and provide the attachments described in Section C of this chapter. In the latter case, complete Item 1 of the “Pre-Application Form;” update, if required, the previous response to Section C Item 10 via an attachment; and comply with the Instructions below.

For every Item below, a response will be provided as a single attachment. Each Item's response should consist of a short overview narrative followed by a summary-level compilation of appropriate supporting documentation comprised of dedicated sets of text and/or citations to and synopses of available complete reports. All supporting documents and reports cited in the application attachment should also be appended to your application. If documents or reports cited in the application are not included at the time of submission or not otherwise readily available, DHS may deem the application incomplete. Note that responses appearing elsewhere in this Application or in other attachments should be cited only (e.g., "See Section X Item Y.Z") and not repeated verbatim.

Each of the Items here relates directly to the evaluation criteria for Certification prescribed in the Act (Sec. 863(d)(2)), i.e., the ATT performs as intended, conforms to the Seller's specifications, and is safe for use as intended.

1. Document and provide all analyses / studies that establish the degree to which the ATT performs as intended:
 - a. When countering an actual terrorist attack. Consider the spectrum of postulated threat scenarios, including both typical and plausible high-loss cases.
 - b. When countering a falsely perceived terrorist attack, i.e., false positive.
 - c. When employed or in standby mode in anticipation of a potential terrorist attack.
2. Document and provide all analyses / studies that establish the degree to which the ATT conforms to Seller specifications.
3. Document and provide all safety and hazard analyses / studies pertinent to the ATT:
 - a. When used as intended, while countering an actual terrorist attack.
 - b. When used as intended, while countering a falsely perceived terrorist attack, i.e., false positive.
 - c. When used as intended, while employed or in standby mode in anticipation of a potential terrorist attack.
 - d. When inadvertently used improperly, while countering an actual terrorist attack.
 - e. When inadvertently used improperly, while countering a falsely perceived terrorist attack, i.e., false positive.
 - f. When inadvertently used improperly, while employed or in standby mode in anticipation of a potential terrorist attack.

E. APPLICANT ACKNOWLEDGEMENT

By signing the Application, the Seller's Authorized Representative certifies the Seller's commitment to provide any additional information requested by DHS to process and evaluate the Application. The Authorized Representative also attests to the completeness and accuracy of the Application and subsequent information supplied.

The following language from the Rule applies:

“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.”

IV. APPLICATION FORMS

A. REGISTRATION

Important: Read carefully and comply precisely with the related Instructions in Chapter III, Section A.

1. INITIAL REGISTRATION UPDATED REGISTRATION

Assigned "SAFETY Act Applicant ID": _____

2. APPLICANT (i.e., SELLER / COMPANY) INFORMATION

a. NAME _____

b. DATA UNIVERSAL NUMBERING SYSTEM (DUNS) NUMBER _____

c. NORTH AMERICAN INDUSTRY CLASSIFICATION SYSTEM (NAICS) CODE _____

d. ADDRESS: Line 1: _____

Line 2: _____

State / Province: _____ Country: _____ Zip Code / Mail Code: _____

e. TELEPHONE NUMBER _____

f. FACSIMILE NUMBER _____

g. E-MAIL ADDRESS _____

h. WEB SITE URL _____

3. PRINCIPAL POC INFORMATION

a. NAME _____

b. ADDRESS: Line 1: _____

Line 2: _____

State / Province: _____ Country: _____ Zip Code / Mail Code: _____

c. TELEPHONE NUMBER _____

d. FACSIMILE NUMBER _____

e. E-MAIL ADDRESS _____

f. E-mail Communication Authorization: Yes No

B. PRE-APPLICATION

Important: This “Pre-Application Form” must be filled out if you are submitting a Pre-Application only, or if you are applying for Designation only, or if you are applying simultaneously for Designation and Certification. Carefully read and adhere to Section B Item 1.b in the Instructions presented in Chapter III.

Important: Read carefully and comply precisely with all of the related Instructions in Chapter III, Section B.

-
1. a. APPLICANT ID: _____ REGISTRATION INFO REMAINS VALID? Yes
- b. APPLICATION TYPE
- Pre-application
 - Designation as Qualified Anti-Terrorism Technology
 - Designation + Certification as an Approved Product for Homeland Security
 - Certification only; DHS Designation Number _____
 - ATT, specifications, level of effectiveness, and use have not changed since Designation
 - Insurance premium and coverage have not changed since Designation
- c. Brief non-proprietary description of ATT is attached? Yes
-

2. ATT DESCRIPTION

- a. NAME _____ MAKE _____ MODEL _____
- b. Brief Executive Summary of ATT is attached? Yes
- c. Similar to another QATT? No Yes
DHS Designation/Certification Number _____
- d. BEING PROCURED BY A FEDERAL AGENCY? No Yes
- i. FEDERAL AGENCY _____
 - ii. POC NAME _____
 - iii. ADDRESS: Line 1: _____
Line 2: _____
State / Province: _____ Country: _____ Zip Code / Mail Code: _____
 - iv. TELEPHONE NUMBER _____
 - v. FACSIMILE NUMBER _____
 - vi. E-MAIL ADDRESS _____

3. a. What technological elements comprise the ATT? _____

b. What external technological elements are essential? _____

4. a. What is the primary means of terrorist attack that the ATT counters?

- Radiation / nuclear Chemical Warfare Humans, e.g., suicide bombers
- Conventional explosives or incendiary weapons to include improvised explosives
- Biological against people, livestock, or agriculture
- Cyber / information technology, especially Information Assurance

b. By what means does the ATT defend against terrorism?

- Deter terrorism Detect activity Identify activity Interdict before attack
 Defeat attack Reduce effects Recover following attack Forensic / investigative

c. What are the most relevant means that terrorists could employ to counter the ATT?

- Inspection or familiarity Trial & error Insider information or action None

d. What are the targets of the terrorist attacks that the ATT defends against?

Primary: _____ Secondary: _____

5. a. Select all potential users of the technology, as an ATT or otherwise.

- Federal Government State/Local Government Non-profit Commercial
 International border / air & sea travel Other

b. Select all current or past users of the technology, as an ATT or otherwise.

- Federal Government State/Local Government Non-profit Commercial
 International border / air & sea travel Other None

6. a. What is the ATT's current state of maturity? _____

b. What is the status of the least mature of any external but essential elements?

- Currently widely deployed or available Limited current deployment or availability
 Unavailable, Projected availability date: _____ No external essential elements

c. How quickly could the ATT, including external elements, be deployed throughout the entire identified market in defense of the U.S.? In a limited few select situations?

- | | | | |
|----------------|--|-----------------|--|
| <u>Entire:</u> | <input type="checkbox"/> 0 – 4 months | <u>Limited:</u> | <input type="checkbox"/> 0 – 4 months |
| | <input type="checkbox"/> 5 – 12 months | | <input type="checkbox"/> 5 – 12 months |
| | <input type="checkbox"/> 1 – 2 years | | <input type="checkbox"/> 1 – 2 years |
| | <input type="checkbox"/> More than 2 years | | <input type="checkbox"/> More than 2 years |

7. Characterize any insurance coverage of the Applicant (i.e., Seller) that might apply in the event of a terrorist action where the technology is (or is to be) deployed:

- a. Current:** Past coverage, but none presently
 No past and no present coverage
 Actively seeking but cannot acquire coverage

Insurer: _____ Occurrence & Annual Aggregate Limits: _____
Annual premium: _____ Deductible/Retention: _____ Exclusions: _____

- b. Additional Quotes:** None Actively seeking but cannot acquire quotes

Insurer: _____ Occurrence & Annual Aggregate Limits: _____
Annual premium: _____ Deductible/Retention: _____ Exclusions: _____

8. Characterize any estimates of the potential liability faced by the Applicant (i.e., Seller) if the ATT were to be marketed without SAFETY Act protections.

- a.** None available

b. Estimated Liabilities (Then-Year U.S. Dollars):

- | | | |
|---|-------------------|--------------------------------------|
| <input type="checkbox"/> Economic damages | Typical: \$ _____ | <u>Plausible High-Loss:</u> \$ _____ |
| <input type="checkbox"/> Punitive damages | Typical: \$ _____ | <u>Plausible High-Loss:</u> \$ _____ |
| <input type="checkbox"/> Other damages | Typical: \$ _____ | <u>Plausible High-Loss:</u> \$ _____ |

9. How are any available estimates of the effect of liability limitations on the profitability of the ATT expressed?

a. None available

b. If the ATT were to be marketed without SAFETY Act protections?

Internal rate of return Dollar cost per unit sold Risk-adjusted rate of return Other

c. If the ATT were to be marketed with SAFETY Act protections?

Internal rate of return Dollar cost per unit sold Risk-adjusted rate of return Other

10. Characterize the business plan elements that have been established for the ATT.

a. None established

b. Current market: Size (Then-year U.S. \$M) \$____M Applicant's share ____%

c. Potential market: Size (Then-year U.S. \$M) \$____M Applicant's share ____%

d. Support deployment expectations presented in Item 6.c? Yes No

e. Sufficient supporting expertise/resources for expectations presented in Item 6.c?

Existing Planned Unplanned

11. Indicate the source of any studies that assess, either quantitatively or qualitatively, the magnitude of risk exposure to the public if the technology:

a. Were not to be deployed as an ATT.

None Own company Independent insurance or risk analysis organizations

b. Were to be deployed as an ATT.

None Own company Independent insurance or risk analysis organizations

12. a. Indicate the estimated potential magnitude of harm to the public if the technology were not deployed as an ATT and there was a terrorist attack.

| | <u>Fatalities</u> | <u>Injuries</u> | <u>Economic Losses</u> | <u>Physical Damage</u> | <u>Mass Disruption</u> | <u>Symbolic Damage</u> |
|----------------|-------------------|-----------------|------------------------|------------------------|------------------------|------------------------|
| Typical Case | _____ | _____ | _____ | _____ | _____ | _____ |
| High-Loss Case | _____ | _____ | _____ | _____ | _____ | _____ |

b. Indicate the percentage decrease in the potential magnitude of harm to the public if the ATT were deployed and there was a terrorist attack.

| | <u>Fatalities</u> | <u>Injuries</u> | <u>Economic Losses</u> | <u>Physical Damage</u> | <u>Mass Disruption</u> | <u>Symbolic Damage</u> |
|----------------|-------------------|-----------------|------------------------|------------------------|------------------------|------------------------|
| Typical Case | _____ | _____ | _____ | _____ | _____ | _____ |
| High-Loss Case | _____ | _____ | _____ | _____ | _____ | _____ |

13. Select the psychological impacts that might well arise from a serious terrorist attack against targets defended by the ATT.

- Regional/national drop in economic activity or property values
- Regional/national drop in social activity sectors, e.g., enjoying public areas, entertainment events, or travel
- Undermining trust in availability or safety of essential infrastructures, social services, or people
- Dread of exposure to a severe hazard, e.g., disease or nuclear radiation
- Loss of something of irreplaceable symbolic or natural value
- Widespread personal fear of potential harm
- Other significant psychological impacts on a large segment of society
- None

14. Indicate the analytical measures that have been established for evaluating the expected operational performance of the ATT.

- None Objectives Functions Metrics Metrics & specific criteria

15. Indicate the means that have been established for monitoring and assessing the performance of the technology after it were to be deployed as an ATT?

- None Periodic inspections Periodic tests or exercises Red team ‘attacks’
 Built-in diagnostics / reporting systems Analytical or indirect indicators

16. Indicate the estimated potential magnitude of harm to the public that the ATT by itself could be responsible for were it to be employed: (a) in response to a terrorist attack; (b) against a falsely perceived terrorist attack, i.e., false positive; and (c) in a standby or alert mode in anticipation of a potential terrorist attack.

| <u>Fatalities</u> | <u>Injuries</u> | <u>Economic Losses</u> | <u>Physical Damage</u> | <u>Mass Disruption</u> | <u>Symbolic Damage</u> |
|-------------------|-----------------|------------------------|------------------------|------------------------|------------------------|
| a. _____ | _____ | _____ | _____ | _____ | _____ |
| b. _____ | _____ | _____ | _____ | _____ | _____ |
| c. _____ | _____ | _____ | _____ | _____ | _____ |

17. Characterize the scientific studies or other corroborative evidence that demonstrate that the technology has substantial utility and effectiveness as an ATT, or that otherwise would support an assessment of the capability of the technology to substantially reduce risks of harm.

a. Reports of analyses or test results

- None Own company Independent organizations

b. Addressing utility and effectiveness

- None While countering a terrorist attack In the absence of a terrorist attack

c. Addressing safety

- None While countering a terrorist attack In the absence of a terrorist attack

d. Addressing other specific performance metrics

- | | |
|--|---|
| <input type="checkbox"/> None | <input type="checkbox"/> Success probability / Expected degree of success |
| <input type="checkbox"/> False positive/negative rates | <input type="checkbox"/> Sensitivity to user error |
| <input type="checkbox"/> Reliability | <input type="checkbox"/> Availability |
| <input type="checkbox"/> Maintainability | <input type="checkbox"/> Robustness |
| <input type="checkbox"/> Interoperability | <input type="checkbox"/> Learning curve and retention |
| <input type="checkbox"/> Quality control/assurance | <input type="checkbox"/> Countermeasures |

e. Demonstrating compliance with specific design or performance standards

- None Industry Government DHS Other

18. Characterize the existing evidence that demonstrates that the ATT has substantial utility and effectiveness in specific aspects of operational performance:

- a. Mission success in representative operational settings _____
- b. System reliability and availability in representative settings _____
- c. Safety for operators, support personnel, or other parties _____
- d. Maintenance, calibration, fault detection / warning / diagnostics, and general sustainability in operational settings _____
- e. Likely countermeasures to be employed by terrorists _____
- f. Adequacy of the concept of operations for use as intended _____
- g. Ability to upgrade or remove a deployed technology _____
- h. Availability and training of operational and support personnel _____

19. Characterize the actual use or testing evidence that demonstrates that the ATT has substantial utility and effectiveness against specific terrorist threats:

- a. Radiation / nuclear _____
- b. Chemical _____
- c. Conventional explosives _____
- d. Biological _____
- e. Cyber/Information Technology _____
- f. Human _____

20. Characterize the actual use or testing evidence that demonstrates that the ATT has substantial utility and effectiveness in defending specific assets:

- a. People _____
 - b. Infrastructure/Capabilities _____
 - c. Buildings/Facilities _____
 - d. Vehicles _____
 - e. Other _____
- Explanatory attachment added? Yes
-

C. DESIGNATION

Important: This section is pertinent if you are applying for Designation only, or if you are applying simultaneously for Designation and Certification. In either case, you must also complete the preceding “Pre-Application Form” in Section B of this chapter.

Add appropriate attachments that are explicitly linked to each of the individual Items 1 – 14 in Section C of Chapter III.

D. CERTIFICATION

Important: This section is pertinent if you are applying simultaneously for Designation and Certification, or if you are applying for Certification only. In the former case, you must also complete the preceding “Pre-Application Form” in Section B of this chapter, and provide the attachments required for Section C of this chapter. In the latter case, complete Item 1 of the “Pre-Application Form;” update, if required, the previous response to Section C Item 10 via an attachment; and comply with the Instructions below.

Add appropriate attachments that are explicitly linked to each of the individual Items 1 – 3 in Section D of Chapter III.

E. APPLICANT ACKNOWLEDGMENTS

Under penalty of perjury, I declare, to the best of my knowledge and belief, that all statements made and information provided in this Application and any accompanying documents are true, correct, and complete.

Prepared By: _____

Title (if applicable): _____

Signature: _____

Date: _____

The signature of the preparer must be notarized below:

APPENDIX – PUBLIC LAW 107-296 "HOMELAND SECURITY ACT OF 2002"

Subtitle G—Support Anti-terrorism by Fostering Effective Technologies Act of 2002

SEC. 861. SHORT TITLE.

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

SEC. 862. ADMINISTRATION.

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

(b) DESIGNATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGIES.

—The Secretary may designate anti-terrorism technologies that qualify for protection under the system of risk management set forth in this subtitle in accordance with criteria that shall include, but not be limited to, the following:

- (1) Prior United States Government use or demonstrated substantial utility and effectiveness.
- (2) Availability of the technology for immediate deployment in public and private settings.
- (3) Existence of extraordinarily large or extraordinarily unquantifiable potential third party liability risk exposure to the Seller or other provider of such anti-terrorism technology.
- (4) Substantial likelihood that such anti-terrorism technology will not be deployed unless protections under the system of risk management provided under this subtitle are extended.
- (5) Magnitude of risk exposure to the public if such antiterrorism technology is not deployed.
- (6) Evaluation of all scientific studies that can be feasibly conducted in order to assess the capability of the technology to substantially reduce risks of harm.
- (7) Anti-terrorism technology that would be effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat or respond to such acts.

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

SEC. 863. LITIGATION MANAGEMENT.

(a) FEDERAL CAUSE OF ACTION.—

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

(2) JURISDICTION.—Such appropriate district court of the United States shall have original and exclusive jurisdiction over all actions for any claim for loss of property, personal injury, or death arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller.

(b) SPECIAL RULES.—In an action brought under this section for damages the following provisions apply:

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

(2) NONECONOMIC DAMAGES.—

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

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

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

(d) GOVERNMENT CONTRACTOR DEFENSE.—

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

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

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

(e) EXCLUSION.—Nothing in this section shall in any way limit the ability of any person to seek any form of recovery from any person, government, or other entity that—(1) attempts to commit, knowingly participates in, aids and abets, or commits any act of terrorism, or any criminal act related to or resulting from such act of terrorism; or (2) participates in a conspiracy to commit any such act of terrorism or any such criminal act.

SEC. 864. RISK MANAGEMENT.

(a) IN GENERAL.—

(1) LIABILITY INSURANCE REQUIRED.—Any person or entity that sells or otherwise provides a qualified anti-terrorism technology to Federal and non-Federal Government customers (“Seller”) shall obtain liability insurance of such types and in such amounts as shall be required in accordance with this section and certified by the Secretary to satisfy otherwise compensable third-party claims arising out of,

relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act.

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

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

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

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

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

(b) **RECIPROCAL WAIVER OF CLAIMS.**—The Seller shall enter into a reciprocal waiver of claims with its contractors, subcontractors, suppliers, vendors and customers, and contractors and subcontractors of the customers, 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 or response or recovery from such act.

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

SEC. 865. DEFINITIONS.

For purposes of this subtitle, the following definitions apply:

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

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

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

(i) is unlawful;

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

(iii) uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.

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

(4) LIABILITY INSURANCE.—

(A) IN GENERAL.—The term “liability insurance” means insurance for legal liabilities incurred by the insured resulting from—

(i) loss of or damage to property of others;

(ii) ensuing loss of income or extra expense incurred because of loss of or damage to property of others;

(iii) bodily injury (including) to persons other than the insured or its employees; or

(iv) loss resulting from debt or default of another.

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

(6) NON-FEDERAL GOVERNMENT CUSTOMERS.—The term “non-Federal Government customers” means any customer of a Seller that is not an agency or instrumentality of the United States Government with authority under Public Law 85–804 to provide for indemnification under certain circumstances for third-party claims against its contractors, including but not limited to State and local authorities and commercial entities.