

**SAFETY Act SUPPORTING STATEMENT FOR
PAPERWORK REDUCTION ACT 1995 SUBMISSIONS**

General Instructions

A Supporting Statement, including the text of the notice to the public required by 5 CFR 1320.5(a)(i)(iv) and its actual or estimated date of publication in the Federal Register, must accompany each request for approval of a collection of information. The Supporting Statement must be prepared in the format described below, and must contain the information specified in Section A below. If an item is not applicable, provide a brief explanation. When Item 17 of the OMB Form 83-I is checked "yes", Section B of the Supporting Statement must be completed. OMB reserves the right to require the submission of additional information with respect to any request for approval.

Specific Instructions

A. Justification

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information.

Public Law 107296, sections 861-865 (See Attachment A)

The Secretary for Homeland Security is responsible for the review and approval of anti-terrorism 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. Under the Regulations, 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. Pursuant to the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, 6 U.S.C. §§ 441-444 (the "SAFETY Act"), and the regulations implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, 6 C.F.R. Part 25, 71 Fed. Reg. 33147, 33159 (June 8, 2006) (the "Regulations"), the Secretary of the U.S. Department of Homeland Security has delegated his responsibilities, powers and functions under the SAFETY Act to the Under Secretary for Science and Technology of the Department.

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

Applications are received from business institutions, for-profit organizations, and State, Local and Tribal Government entities. Applications are reviewed for benefits, technology/program evaluations, and regulatory compliance. The Under Secretary may designate anti-terrorism technologies that qualify for liability protections under the system of risk management set forth in the regulations in accordance with specific criteria. Anti-terrorism technologies are reviewed and approved by the Under Secretary. If approved, the Under Secretary will issue SAFETY Act protections to the Seller and place the anti-terrorism technology on an Approved Product List for Homeland Security.

3. Describe whether, and to what extent, the collection of information involves

SAFETY ACT SUPPORTING STATEMENT A

the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.

Information Technology is used in the collection to reduce the data gathering and records management burden. S&T uses a secure website to collect all of the SAFETY Act Application Forms information. The SAFETY Act Web site, www.safetyact.gov, uses a secure system of fillable forms that the Applicant completes, signs digitally, and submits to the SAFETY Act Office for evaluation.

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purposes described in Item 2 above.

The collection of SAFETY Act Application Kit information was based on new legislation which identified the need for the federal government to collect critical information regarding technologies that could benefit Homeland Security initiatives.

5. If the collection of information impacts small businesses or other small entities (Item 5 of OMB Form 83-I), describe any methods used to minimize burden.

S&T developed a streamlined on-line application process that can be saved and updated. It has been deployed to minimize the burden on interested Small Business participants and other applicants. The specifics of the SAFETY Act evaluation process are contained within the Final Rule published in the Federal Register, Vol 71, No.110, June 8, 2006.

6. Describe the consequence to Federal program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

Not collecting this information would make it more difficult, timely and costly for DHS to identify viable anti-terrorism technologies. Collecting it less frequently would result in the review of fewer anti-terrorism technologies resulting in the issuance of fewer SAFETY Act protections and ultimately fewer anti-terrorism technologies to protect the Homeland.

SAFETY ACT SUPPORTING STATEMENT A

7. Explain any special circumstances that would cause an information collection to be conducted in a manner:
- Requiring respondents to report information to the agency more often than quarterly;
 - requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it;
 - requiring respondents to submit more than an original and two copies of any document;
 - requiring respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records for more than three years;
 - In connection with a statistical survey, that is not designed to produce valid and reliable results that can be generalized to the universe of study;
 - requiring the use of a statistical data classification that has not been reviewed and approved by OMB;
 - that includes a pledge of confidentiality that is not supported by authority established in statute or regulation, that is not supported by disclosure and data security policies that are consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use; or
 - requiring respondents to submit proprietary trade secret, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law.

As part of the SAFETY Act Evaluation process, some Applicants may choose to submit sensitive but unclassified materials. All sensitive but unclassified material is safeguarded as outlined in Department of Homeland Security Management Directive System MD Number 11042.1. (Attached in ROCIS)

SAFETY ACT SUPPORTING STATEMENT A

8. If applicable, provide a copy and identify the data and page number of publication in the Federal Register of the agency's notice, required by 5 CFR 1320.8(d), soliciting comments on the information collection prior to submission to OMB. Summarize public comments received in response to that notice and describe actions taken by the agency in response to these comments. Specifically address comments received on cost and hour burden.

See Attachment (60-Day Notice, 2 pages; 30-Day Notice, 2 pages). DHS S&T did not receive any comments as a result of the 60-Day notice, which ended October 16, 2006.

Describe efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.

NONE.

Consultation with representatives of those from whom information is to be obtained or those who must compile records should occur at least once every 3 years -- even if the collection of information activity is the same as in prior periods. There may be circumstances that may preclude consultation in a specific situation. These circumstances should be explained.

NONE.

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

NONE.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.

Department of Homeland Security, Office of the Secretary, 6 CFR Part 25 (USCG-2003-15425) PIN 1601-AA15 Regulations Implementing the Support Anti-terrorism by fostering Effective Technologies Act of 2002 (the SAFETY Act) Paragraph 25.10.

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private. This justification should include the reasons why the agency considers the questions necessary, the specific uses to be made of the information, the explanation to be given to person's form whom the information is requested, and any steps to be taken to obtain their consent.

NONE.

SAFETY ACT SUPPORTING STATEMENT A

12. Provide estimates of the hour burden of the collection of information. The statement should:

- Indicate the number of respondents, frequency of response, annual hour burden, and an explanation of how the burden was estimated. Unless directed to do so, agencies should not conduct special surveys to obtain information on which to base hour burden estimates. Consultation with a sample (fewer than 10) of potential respondents is desirable. If the hour burden on respondents is expected to vary widely because of differences in activity, size, or complexity, show the range of estimated hour burden, and explain the reasons for the variance. Generally, estimates should not include burden hours for customary and usual business practices.

Number of annual respondents: 2500
Frequency of response (per respondent): One
Annual hour burden: 121,400 hours
% On line 100%

This annual burden was estimated based on the average time it takes a respondent to complete the SAFETY Act Application. The SAFETY Act Application Kit has ten forms that require approx 48.5 hours to complete. Each form has a varying degree of difficulty and the associated burden hours for each form are noted on the form.

- If this request for approval covers more than one form, provide separate hour burden estimates for each form and aggregate the hour burdens in Item 13 of OMB Form 83-I.
- Provide estimates of annualized cost to respondents for the hour burdens for collections of information, identifying and using appropriate wage rate categories. The cost of contracting out or paying outside parties for information collection activities should not be included here. Instead, this cost should be included in Item 14.

Average Hourly Rate: \$100.00
Per Application Kit Cost Burden: \$4,850.00
Annual cost burden: \$12,140,000

SAFETY ACT SUPPORTING STATEMENT A

13. Provide an estimate of the total annual cost burden to respondents or record keepers resulting from the collection of information. (Do not include the cost of any hour burden shown in Items 12 and 14).

- The cost estimate should be split into two components: (a) a total capital and start-up cost component (annualized over its expected useful life);

NONE.

and (b) a total operation and maintenance and purchase of services component. The estimates should take into account costs associated with generating, maintaining, and disclosing or providing the information. Include descriptions of methods used to estimate major cost factors including system and technology acquisition, expected useful life of capital equipment, the discount rate(s), and the time period over which costs will be incurred. Capital and start-up costs include, among other items, preparations for collecting information such as purchasing computers and software; monitoring, sampling, drilling and testing equipment; and record storage facilities.

NONE.

- If cost estimates are expected to vary widely, agencies should present ranges of cost burdens and explain the reasons for the variance. The cost of purchasing or contracting out information collection services should be a part of this cost burden estimate. In developing cost burden estimates, agencies may consult with a sample of respondents (fewer than 10), utilize the 60-day pre-OMB submission public comment process and use existing economic or regulatory impact analysis associated with the rulemaking containing the information collection, as appropriate.

N/A

- Generally, estimates should not include purchases of equipment or services, or portions thereof, made: (1) prior to October 1, 1995, (2) to achieve regulatory compliance with requirements not associated with the information collection, (3) for reasons other than to provide information or keep records for the government or (4) as part of customary and usual business or private practices.

N/A

14. Provide estimates of annualized cost to the Federal government. Also, provide a description of the method used to estimate cost, which should include quantification of hours, operational expenses (such as equipment, overhead, printing, and support staff), and any other expense that would not have been incurred without this collection of information. Agencies also may aggregate cost estimates from Items 12, 13, and 14 in a single table.

The annualized SAFETY Act operating cost is approximately \$5.5M.

SAFETY ACT SUPPORTING STATEMENT A

15. Explain the reasons for any program changes or adjustments reporting in Items 13 or 14 of the OMB Form 83-I.

All form changes were made by DHS S&T to reduce the cost and time burden to the public.

16. For collections of information whose results will be published, outline plans for tabulation, and publication. Address any complex analytical techniques that will be used. Provide the time schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

NONE.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons that display would be inappropriate.

NONE.

18. Explain each exception to the certification statement identified in Item 19, "Certification for Paperwork Reduction Act Submission," of OMB 83-I.

NONE.

Attachment A(1)

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

SAFETY ACT SUPPORTING STATEMENT A

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—

SAFETY ACT SUPPORTING STATEMENT A

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

SEC. 864. RISK MANAGEMENT.

(a) IN GENERAL.—

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

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

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

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

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

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

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

SAFETY ACT SUPPORTING STATEMENT A

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.