December 15, 2003

Via Electronic Submission

Docket Management Facility
U.S. Department of Transportation
400 7th Street, S.W.
Washington, D.C. 20590-0001

Re: Comments on Interim Regulations Implementing the SAFETY Act
Docket Number USCG-2003-15425

Dear Sir or Madam:

On behalf of the Section of Public Contract Law of the American Bar Association (“the Section”), we are submitting comments on the Interim Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (“SAFETY Act”). The Section consists of lawyers having interest and expertise in the area of public procurement both within Government and in the private sector. The members of the Section are all concerned with the fair and efficient operation of the procurement process.

The views expressed herein have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and, therefore, should not be construed as representing the policy of the Association as a whole.
We appreciate the opportunity to submit these comments.

Sincerely,

[Signature]

Hubert J. Bell, Jr.
Chair, Section of Public Contract Law

Enclosure

cc: Patricia H. Wittie
    Robert L. Schaefer
    Michael A. Hordell
    Patricia A. Meagher
    Mary Ellen Coster Williams
    Norman R. Thorpe
    Council Members
    Steven P. Pfitzer
    Michael F. Mason
    David Kasanow
COMMENTS OF THE AMERICAN BAR ASSOCIATION
SECTION OF PUBLIC CONTRACT LAW

In the matter of

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

Docket No. USCG-2003-15425
U.S. Department of Transportation

Introduction

The American Bar Association Section of Public Contract Law is pleased to submit these comments to the Department of Homeland Security on the interim rule implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act). The views expressed herein have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and, therefore, should not be construed as representing the policy of the Association as a whole.

Background

Following the tragic events of September 11, 2001, the President’s National Strategy on Homeland Security transmitted to Congress on July 16, 2002 recognized the vital role that private sector entities must play in any successful effort to deploy anti-terrorism technologies to protect national security against future acts of terrorism. Companies with significant existing technology and service capabilities, including major defense contractors whose technology and services are used already by the Department of Defense, were not willing to make their technology and services available for homeland security due to the potential exposure for unbounded and uninsurable third party tort liabilities resulting from a terrorist act. The current system of tort law and product liability in the U.S. could result in the imposition of unlimited liability for third party claims.

Historically, when the United States Government has acquired technology and services in support of national defense needs, various mechanisms have been available to protect sellers from unlimited tort liability for high risk undertakings (e.g., development, testing, and deployment of new weapons systems). These mechanisms have included use of government-owned facilities, indemnification of contractors by the United States in certain circumstances, the judicial government contractor defense, or combinations thereof. Nevertheless, as the National Strategy notes, responsibility for homeland security is not and cannot be solely the responsibility of the Federal Government. Indeed, the “frontline” responsibility for many terrorist threats and for securing critical infrastructure, rests with state and local governments, port authorities, or even private entities such as utilities. As a result, in deliberations over the Homeland Security
Act, the administration and Congress determined that a mechanism was needed to manage potential third party liability claims against the providers of anti-terrorism technology and services so that essential existing technology and services could be deployed rapidly and new capabilities could be developed.

In response to these concerns, as part of the creation of the Department of Homeland Security, Congress considered legislation to address the third party liability exposure of sellers of anti-terrorism technology. The SAFETY Act was included in the final Homeland Security bill and signed by the President. As enacted, the SAFETY Act (Subtitle G of Title VIII of the Homeland Security Act, Pub. L. No. 107-296, codified at 6 U.S.C. §§ 441-444) changes the liability regime for Sellers of anti-terrorism technology by, inter alia: (1) limiting potential claims for liability in the event of an act of terrorism to claims only against Sellers, and only when their technology is the “proximate cause” of the claimant’s injuries, thereby eliminating claims against the customers of such Sellers or other third parties; (2) establishing a federal cause of action requiring that any claims seeking damages against Sellers be filed in federal court; (3) providing limitations on punitive damages and prejudgment interest; (4) providing a statutory “government contractor defense;” and (5) capping the potential liability of Sellers of qualified anti-terrorism technology at the amount of the insurance that the Secretary requires Sellers to obtain.

The Interim Rule

The Department of Homeland Security (Department or DHS) issued its interim rule implementing the SAFETY Act on October 16, 2003. The interim rule is effective immediately, but includes a request for comments. Comments are due on December 15, 2003. The interim rule was preceded by a proposed rule issued on July 11, 2003 and a 30-day comment period. DHS indicated in the proposed rule that it intended to act quickly by means of an interim rule to implement the SAFETY Act, while allowing further comments.

The Basis for Comment by the ABA Section of Public Contract Law

The Section of Public Contract Law is uniquely qualified to offer comments on the interim rule. The Section’s members include attorneys from private industry, government, and private practice whose primary area of practice involves public contracts. The Section’s members routinely deal with issues of contractor liability for third party claims in connection with national security programs. Virtually all U.S. government contracts (and many state and local government contracts) contain mandatory provisions addressing insurance and liability for third party claims (See, e.g., 48 C.F.R § 52.228-7). These clauses are unique to government contracts and do not ordinarily appear in commercial contracts. The procurement statutes and regulations also include many different provisions addressing division of liability between the Government and its contractors for matters such as research and development (10 U.S.C. § 2354), ultra-hazardous risks in manufacture and deployment of complex weapons (Pub. L. No. 85-804), environmental remediation (42 U.S.C. § 9619) and others. There is a close tie between the acquisition of anti-terrorism technologies by the Government and how the SAFETY Act will
be reflected in its contracts, e.g., the just-published DHS Acquisition Regulation contains a section on interaction of the procurement process with the SAFETY Act.

The interim rule issued by DHS carefully addresses the provisions of the statute and, recognizing the Secretary’s discretion to provide the benefits of the statute quickly for deployment of critically needed technology, fleshes out key concepts and provides the necessary administrative structure for qualification and certification of products and services. The interim rule reflects careful analysis of the statute, its purpose and the benefits of anti-terrorism technology. DHS has done an excellent job in a very short period of understanding and addressing the complexities of the SAFETY Act – and the significance of technology at all levels for homeland security. The following comments are intended to provide discussion of important procurement-related issues in the spirit of further comment requested by DHS.

I. Implementation Issues

A. Coordination with Pub. L. No. 85-804

Since World War II, Pub. L. No. 85-804 (and its predecessors) has provided authority for indemnification of companies performing U.S. Government contracts involving unusually hazardous and nuclear risks. In contrast to the SAFETY Act’s framework, Public Law 85-804 indemnification does not inhibit actions by third-parties harmed as a result of the contractor’s activities. Instead, the Government analyzes the nature of the risk and the availability of insurance, and then agrees to indemnify the contractor from third party claims by defending actions by third-parties and paying any resulting damages above the insurance coverage required by the Government to be maintained by the contractor.

Implementing regulations at FAR Part 50 state that the authority conferred by Public Law 85-804 may not be relied upon when other adequate legal authority exists within the agency (FAR 50.102(a)(2)), and prohibit contracts, amendments or modifications “unless other legal authority within the agency concerned is deemed to be lacking or inadequate.” (FAR 50.203(b)(2)).

With passage of the SAFETY Act, however, the issue of the availability or adequacy of “other legal authority” may become problematic. Public Law 85-804 indemnification and SAFETY Act protection differ in the scope of their coverage in important ways. Public Law 85-804 authority is available only to contractors performing contracts involving unusually hazardous or nuclear risks for selected Federal agencies. The contractor is indemnified for damages related to the identified risks, and these risks need not be limited to situations involving a terrorist attack. The SAFETY Act, on the other hand, extends liability protection to companies providing anti-terrorism technologies to both Federal Government and non-Federal Government customers. The SAFETY Act’s coverage, however, only applies in the event of a terrorist act.

On February 28, 2003, President George W. Bush issued Executive Order 13286, placing additional conditions on the use of P.L. 85-804 indemnification by authorized Federal agencies when the contractor’s technology is or could be eligible for SAFETY Act coverage. The
Executive Order requires that the Department of Defense first consider SAFETY Act coverage before determining whether Public Law 85-804 indemnification is “necessary for the timely and effective conduct of the United States military or intelligence activities.” Apart from the Department of Defense, other authorized agencies, as a prerequisite to indemnification, must (i) consult the Secretary of the Department of Homeland Security regarding the appropriateness of SAFETY Act coverage, and (ii) obtain approval from the Director of the Office of Management and Budget (OMB) for exercise of indemnification power.

The preamble to the interim rule addresses the relationship of the SAFETY Act to Public Law 85-804 indemnification. In this regard, the preamble states:

The Department recognizes that Congress intended that the SAFETY Act’s liability protections would substantially reduce the need for the United States to provide indemnification under Public Law 85-804 to Sellers of anti-terrorism technologies. Where applicable, the strong liability protections of the SAFETY Act should, in most circumstances, make it unnecessary to provide indemnification to Sellers. The Department recognizes, however, that there might be, in some limited circumstances, technologies or services with respect to which both SAFETY Act coverage and indemnification might be warranted. (Citation to legislative history omitted.)

68 Fed. Reg. at 59694. The preamble thereafter summarizes Executive Order 13286, which it describes as the Administration’s “recognition of this close relationship between the SAFETY Act and indemnification authority.” Id.

The interim rule itself, however, is silent with regard to the interplay between SAFETY Act coverage and Public Law 85-804 indemnification. Neither does it mention Executive Order 13286 or FAR Part 50. Given that Congress was mindful of the existing indemnification authority when it passed the SAFETY Act legislation, and the administration thereafter amended the executive agencies’ indemnification powers as noted above, the absence of a link between Public Law 85-804 and the SAFETY Act protections constitutes a significant gap in the interim rule. Both government agencies and the contracting community would be benefited if DHS were to provide needed guidance regarding:

(a) Under what circumstances the availability of a SAFETY Act designation will not constitute “other adequate legal authority within the agency,” so that both a SAFETY Act designation and indemnification under Public Law 85-804 might be available; and

(b) How the Department will make the determination required by E.O. 13286 regarding whether use of the SAFETY Act is
appropriate when advising civilian agencies pursuant to E.O. 13286;

(c) How the Department will interact with OMB when civilian agencies seek indemnification approval.

In this regard, DHS should amend the interim rule to reflect the following considerations:

(i) Some anti-terrorism technologies involve unusually hazardous risks, independent of acts of terrorism. For example, new vaccines to protect emergency response personnel and citizens from biological attack typically must undergo clinical trials, which are inherently risky to human subjects, before receiving FDA approval for general use. Thereafter, new vaccines present the risk of adverse reactions in a small percentage of the general population. Similarly, companies providing cyber-security services often face the risk of inadvertent damage, loss or disclosure of computer files and personal data, as part of their work performance. In addition, chemical, radiation, and biological detection devices may produce “false positive” readings, which could prove highly disruptive and potentially hazardous in some circumstances. While none of these substantial risks involve an act of terrorism, and would not be covered by the SAFETY Act, each of these technologies may be necessary to protect against a terrorist act. Unless Public Law 85-804 indemnification is available, many companies facing such unusually hazardous risks and the related legal liabilities might not be willing to provide their anti-terrorism products and services.

(ii) Certain companies with especially critical anti-terrorism technologies might demand indemnification, as an absolute pre-condition to selling their anti-terrorism products or services to the Government. In order to acquire especially critical anti-terrorist technologies, authorized agencies should have Public Law 85-804 indemnification available as an additional contracting incentive.

(iii) Safety Act coverage reduces the liability risks from acts of terrorism, and should reduce the cost to the United States of indemnification under Public Law 85-804. When determining whether to provide indemnification, DHS, OMB, and agencies should take into account the reduction in liability for Qualified Anti-terrorism Technologies and
Qualified Products for Homeland Security. Given these liability protections, indemnification should be less costly to the Government for anti-terrorism technologies covered by the SAFETY Act than other, similar products and services.

B. Coordination of SAFETY Act Review with Federal Agency Procurements

The interim rule raises a number of implementation and process questions that may complicate the process for proposing qualified anti-terrorism technologies for federal procurements.

§ 25.3 Designation of Qualified Anti-Terrorism Technology

25.3(f) Content of Designation

**Issue:** The designation is to specify the technology and the Seller(s) of the technology.

Can there be a “combined” designation that would apply to all qualified component technologies incorporated into the designated technology, and to all Sellers of qualified component technologies incorporated into the designated technology? Such a “combined” designation would remove any ambiguity about whether suppliers, subcontractors, and others at a lower tier in the supply chain are covered by a designation.

**Issue:** DHS suggests that the SAFETY Act provides that before designating a qualified anti-terrorism technology, the Secretary must examine the amount of liability insurance the Seller proposes to maintain. The Under Secretary’s designation includes the Under Secretary’s certification of required insurance under § 25.4(h)

Does the Act require the Secretary’s examination and determination of the amount of insurance before the technology is designated, or can the amount of insurance be examined and certified at a later time when the technology actually is produced and deployed?

§ 25.3(g) Coordination with Government Agency Procurements

**Issue:** The Secretary’s designation or lack of designation of a technology should not be the source of an adverse inference in a Federal agency procurement.

Section 25.3(g) of the interim rule states:

*Government procurements.* The Under Secretary may coordinate a SAFETY Act review in connection with a Federal, state or local government agency procurement of an anti-terrorist technology in any manner he or she deems appropriate and consistent with the Act and other applicable laws.
The Discussion section of the Federal Register Notice of the interim rule, at 68 Fed. Reg. 59692, includes these comments on Section 25.3(g):

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

The Department requests public comments regarding the best way for the Department to … coordinate the SAFETY Act review with agency procurements.

The Section’s comments here are directed primarily at Federal agency procurements. Nevertheless, where possible we have also addressed them in light of the ABA’s Model Procurement Code (MPC), which has been adopted in whole or in substantial part by more than 15 States and dozens of local jurisdictions around the country.

The Section believes DHS’s intent to coordinate SAFETY Act reviews with anti-terrorism procurements can facilitate getting such products or services quickly and economically into use. As detailed below, it suggests two clarifications. First, receiving a determination by DHS (or not) is not determinative whether any technology meets the requirements of any particular solicitation. The regulations should expressly acknowledge this. Second, DHS should not use the evaluation process to suggest improvements to antiterrorism technologies and should prohibit any transmission of ideas taken from one submission to others.

Background – Competition requirements

Federal government agencies are required by law to promote full and open competition in their procurements. 10 U.S.C. § 2304; 41 U.S.C. § 253; Federal Acquisition Regulation (FAR), 48 C.F.R. Part 6. See also Federal Aviation Administration (FAA) Acquisition Management System (AMS) § 3.1.3 (goal of the AMS is to encourage competition as the preferred method of contracting); MPC §§ 3-201, 3-203, 3-206. The FAR defines “full and open competition” to mean that all responsible sources are permitted to compete. FAR 2.101. In addition to promoting full and open competition, agencies are required to “only include restrictive provisions or conditions [in their solicitations] to the extent necessary to satisfy the needs of the agency or as authorized by law,” and to state their requirements with respect to an acquisition in terms of functions to be performed, performance required, or essential physical characteristics. FAR 11.002(a)(1), (a)(2). Solicitations containing specifications that are unduly restrictive of
competition are subject to legal challenge. See, e.g., XTRA Lease, Inc. v. United States, 50 Fed.Cl. 612, 624 (2001); Prisoner Transp. Services, LLC; V1 Aviation, LLC; AAR Aircraft Services, B-292179, B-292179.2, B-292179.3, June 27, 2003, 17 CGEN ¶11,496.

Federal agencies are also required to disclose, in each solicitation, the factors that will be used to evaluate proposals. 10 U.S.C. § 2305(a)(2)(A)(i); 41 U.S.C. § 253a(b)(1)(A); FAR 15.304(d); AMS § 3.2.2.2; MPC §§ 3-202(5), 3-203(5). Price and, except where sealed bids are used, past performance are required evaluation factors. FAR 15.304(c). Nevertheless, these factors are often accompanied by one or more “technical” evaluation factors when competitive negotiation is used. Such factors may include management, financial controls, small business subcontracting goals, and well as purely technical considerations such as the likelihood of achieving particular performance criteria. Evaluation of proposals necessarily involves the exercise of judgment. By law, however, that judgment must be exercised within the parameters of the evaluation criteria that are disclosed in the particular solicitation.

Comparison of the purpose of the SAFETY Act

The purpose of the SAFETY Act is to promote the development of technologies that can detect, prevent, or mitigate the effects of acts of terrorism by providing to Sellers of such technologies relief from certain types of potential liability. The Act’s purpose is not, however, to define the particular needs of a specific government agency customer, nor should the designation process result in a determination that a particular anti-terrorism technology is suitable for, or meets the requirements of, a particular government agency solicitation. Indeed, DHS is obligated to review applications whether or not they are submitted in the context of a current agency procurement. The SAFETY Act review process and the evaluation process under a specific agency procurement are legally and conceptually separate and, in the view of the Section, should remain clearly separate.

The Department has announced its willingness to “coordinate” its application reviews with government agency procurements, consistent with the Act and other applicable laws (interim rule Sec. 25.3(g)), and it intends to review applications relating to technologies that are the subject of government agency procurements on an “expedited basis” (Discussion of interim rule, Para. 2, 68 Fed. Reg. at 59692). It is appropriate for the Department to be cautious about this process, but subject to the restrictions described below, such coordination is likely to benefit the government procurement process and is thus desirable.

Coordinating the application review process

Coordination of the application review process with government agency procurements raises a number of concerns. First, as noted above, the purpose of a SAFETY Act application review is different from the purpose of an evaluation under a particular government agency procurement. In most instances, government agency procurements must be conducted competitively and must include price and past performance as evaluation factors, but those issues are not directly relevant to a SAFETY Act review. Conversely, a SAFETY Act review must
address factors that would not be appropriate evaluation factors in a government agency procurement, including –

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

- 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.

- Magnitude of risk exposure to the public if such anti-terrorism technology is not deployed.

SAFETY Act, Section 862(b)(3), (4), (5). Although some of these considerations may be included in a government agency’s acquisition planning process, they are outside the control of offerors and thus will not be evaluation factors used to discriminate among the technologies identified in proposals submitted in response to a specific agency solicitation.

This point is particularly significant due to the possibility of an “adverse inference” based on the Department’s determination not to designate a particular technology. Although DHS is obligated to consider “prior U.S. Government use or demonstrated substantial utility and effectiveness” (SAFETY Act, Section 862(b)(2)), those considerations by definition relate to “prior” use and are independent of the specific technical requirements of any current procurement. Moreover, a decision not to designate a particular technology may well be based on factors having nothing to do with the effectiveness of the technology or whether it meets the particular specifications called out in a government solicitation. For example, the Department may decline to designate a technology because it determines that adequate insurance is available to the Seller without such a designation, or that the “magnitude of the risk exposure” is not sufficient to justify granting a designation. Neither of those determinations speak to price, past performance, or the quality, effectiveness, or technical characteristics of the technology in question.

For that reason, the Department must ensure that in “coordinating” its review process with government agency procurements, it expressly refuses to permit any adverse inference about the quality, reliability, or effectiveness of technologies that it chooses not to formally designate as qualified anti-terrorism technologies (QATTs). In the context of agency procurements, a designation should not under any circumstances be considered an endorsement by DHS (or by the federal government) of the particular technology, and the failure to designate a particular technology should not be regarded as reflecting any adverse or unfavorable view of that technology by DHS (or by the federal government). In that regard, the Section recommends that the following additional clause be included in the interim rule:

A determination by the Under Secretary to designate, or not designate, a particular technology as a qualified anti-terrorism
technology, is not a determination that the technology meets, or fails to meet, the requirements of any solicitation issued by any federal government customer or non-federal government customer. All determinations by the Secretary with respect to technologies submitted for review, are based on the factors identified in Section 25.3(b), and are made independent of, and without regard to, the specific terms, conditions, specifications, statements of work, or evaluation factors included in particular procurements.

§ 25.4 Obligations of Seller

25.4(e) Reciprocal Waiver of Claims

**Issue:** The Seller is required to enter into a reciprocal waiver of claims with its contractors, subcontractors, suppliers, vendors, and customers, and contractors and subcontractors of the customer, involved in the manufacture, sale, use, or operation of qualified technologies.

Does the reciprocal waiver apply to the federal government as a customer? What happens if reciprocal waivers are not obtained from U.S. government agencies?

25.4(i) Seller’s Continuing Obligation

**Issue:** DHS requires that each year after a certification of approval, the Seller must certify to the Under Secretary that the Seller has maintained the required insurance.

The annual certification is unnecessary. Federal contracting agencies have worked diligently in recent years to remove unnecessary and burdensome certifications from the procurement process. This requirement in the interim rule is a regression. DHS should remove this certification. DHS could require Sellers to advise the Department if insurance coverage is terminated, lapses, or is reduced in any manner, and appropriate measures concerning the Seller’s designation could then be taken. The addition of an annual certification adds no further protection but does impose a barrier to sellers in considering whether to make their technologies available.

§ 25.5 Procedures for Designation of Qualified Anti-terrorism Technologies

25.5(d) Recommendation of the Assistant Secretary

**Issue:** The review process is conducted by the Assistant Secretary, and within 90 days after receipt of a complete application, the Assistant Secretary is to make a recommendation on Designation to the Under Secretary.

Rather than this multi-layered bureaucratic process, should the Assistant Secretary make the decision on designation, instead of a recommendation, with an applicant having an appeal right to the Under Secretary on an adverse decision?
**25.5(e) Action by the Under Secretary**

**Issue:** The Under Secretary has 30 additional days after the Assistant Secretary’s recommendation in which to make the Designation.

Are 30 additional days needed? Should the Under Secretary be required to make a decision in a shorter period of time (e.g., within 7-10 days)?

Should the Assistant Secretary’s recommendation become final, if not acted upon by the Under Secretary within the allotted time?

**Issue:** “The Under Secretary’s decision shall be final and not subject to review, except at the discretion of the Under Secretary.”

It is not clear why DHS is so resistant to even a limited review of the Under Secretary’s decision. 68 Fed. Reg. at 59688. Given the length of the process that DHS has constructed for its applications, an opportunity for review should be considered – certainly it could be carved out of timeframes already set forth in the interim rule without lengthening the process further. Given that DHS intends to make use of national laboratories, Federally Funded Research and Development Centers, and consultants, it would be prudent to consider the possibility that errors, communication failures, and other bureaucratic confusion could prevent important technologies from being designated. A review process that allows an applicant to understand the basis for the designation and, potentially, point out errors, or bring information to light that may not have been properly considered would advance the purposes of the statute. DHS has suggested that a review process is not appropriate because the designation decisions are “discretionary.” Administrative Boards and courts review discretionary decisions regularly under the Administrative Procedure Act’s arbitrary and capricious standard. Most of the Government’s decisions are upheld, but errors and poor decisions do occur and have been overturned. So long as a review process does not become an unnecessarily complex and time consuming endeavor, it would provide transparency and a guarantee of basic fairness to the process.

**II. Government Contractor Defense**

The interim rule addresses the government contractor defense in Sections 25.6 and 25.7. The commentary on the government contractor defense contains important points that need to be addressed in the regulations. These comments are provided pursuant to the express request in the interim rule for further comment on the government contractor defense.

**A. Explain the Prerequisites for Applicability of the Defense**

(1) **Defense Should Arise Automatically Upon Certification.**

The SAFETY Act provides:

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 . . . 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. § 863(d).

The commentary on the interim rule (68 Fed. Reg. 59688) and statements in the legislative history of the statute (148 Cong. Rec. E2080 (statement of Rep. Armey)) indicate that the companies will have a government contractor defense as it was in existing law at the date of enactment. These references to the judicial government contractor defense as of the date of enactment create a potential ambiguity or inconsistency because the elements of the defense applicable to certified anti-terrorism technologies are not contained in the statute or in the interim rule.

Absent the statute, a government contractor is entitled to the protection of the judicially-created government contractor defense where the following three elements show that the government has exercised a “discretionary function” with respect to the matter causing injury: (i) officials of the United States Government approved reasonably precise specifications for the product or service; (ii) the equipment conformed to those specifications; and (iii) the supplier of the goods or services had warned the Government about any latent dangers in the use of goods or services actually known to the contractor but not to the United States. Boyle v. United Technologies Corp., 487 U.S. 500, 512 (1988). The commentary to the interim rule notes that these elements are simply inapplicable, and generally would not be provable, in the context of the statutory defense:

While the government contractor defense is a judicially-created doctrine, Section 863’s express terms supplant many of the requirements in the case law for application of the defense. . . . Sellers of qualified anti-terrorism technologies need not design their technologies to federal government specifications in order to obtain the government contractor defense under the SAFETY Act. Instead, the Act sets forth criteria for the Department’s ‘approval’ of technologies. . . . This express statutory framework thus governs in lieu of the requirements developed in case law for the application of the government contractor defense. . . . Procedurally, the presumption of applicability of the government contractor defense is conferred by the Secretary’s ‘approval’ of a qualified anti-terrorism technology specifically for the purposes of the government contractor defense. 68 Fed. Reg. at 59691-59692.

These points should be made in the regulations. The regulations should be clear that the Seller need not prove anything more than that it has received the certification for the anti-terrorism technology at issue in the litigation. The statutory defense arises from the fact that the product has been certified by the Secretary as an Approved Product for Homeland Security. This is very different from the judicial government contractor defense, which requires the contractor
to prove that the Government exercised discretion with respect to the specifications for the product and that the contractor warned of known, latent defects. The statutory defense arises automatically as a result of that certification and bars any claims, unless the defense is defeated under the specific and limited circumstances (fraud in procuring the certification) discussed below.

(2) Regulatory Amendment

Section 25.6 of the interim rule should be amended to include the following new subsection:

([1]) Upon the issuance of the certification pursuant to [subsection (_) of this regulation], a Seller of a product or service containing the approved technology is entitled to a statutory ‘government contractor defense’ to civil liability. The statutory defense arises from the fact that the product or service has been certified by the Secretary as an Approved Product for Homeland Security. The defense arises automatically as a result of the certification and bars any claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies approved by the Secretary have been deployed in defense against or response or recovery from such act. No further showing is required.

B. Prescribe the Scope of the Defense

(1) Claims Affected

The commentary states:

While the Act does not expressly delineate the scope of the defense (i.e., the types of claims that the defense bars), the Act and the legislative history make clear that the scope is broad. For example, it is clear that any Seller of an ‘approved’ technology cannot be held liable under the Act for design defects or failure to warn claims, unless the presumption of the defense is rebutted by evidence that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the course of the Secretary’s consideration of such technology. 68 Fed. Reg. at 59691.

This essential point concerning the breadth of the statutory defense should be incorporated in the regulations themselves. The history of the government contractor defense since the Supreme Court first recognized it in the Boyle case includes extensive litigation over the meaning and breadth of the defense. Clarity on that subject in these regulations could serve to avoid much unnecessary litigation. Thus the Section recommends that the regulations should
be explicit in defining the scope of the defense broadly to include all potential asserted theories of liability. Such an approach is consistent with the draft commentary and other portions of the regulations which state that the defense applies to design defect and failure to warn claims.

This approach is supported by *Boyle* and its progeny. *Boyle* was a design defect case. In extending the judicially-created government contractor defense to failure-to-warn claims, the courts of appeals have uniformly recognized that the same practical concerns for the efficiency and effectiveness of the contracting process are at stake, whatever state-law tort theory a claimant invokes. That reasoning, in turn, supports the extension of the statutory defense to all other theories of liability.

(2) **Applicability to Non-Federal Sales**

The regulations also should expressly incorporate the principle that the statutory defense is not confined to products and services that are sold to the federal government pursuant to a federal procurement and would extend to sales to state and local governments as well as private parties, even though the judicially created government contractor defense is so limited. The statute states:

> 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. § 863(d).

The commentary explains that “the government contractor defense is available not only to government contractors, but also to those who sell to state and local government and the private sector.” 68 Fed. Reg. at 59691. The term “non-Federal Government customers” in the statute is expansive, but could bear some clarification in the regulations.

(3) **Recommended Amendment**

The following language is proposed as a new subsection in proposed § 25.6 of the regulations:

> ([2]) The government contractor defense bars any claim for relief, however denominated, against a Seller of a product or service containing qualified anti-terrorism technologies that are certified for inclusion on the Approved Products List, including claims for

---

1. *See, e.g., Oliver v. Oshkosh Truck Corp.*, 96 F.3d 992, 1003 (7th Cir. 1996) (“The defense applies to failure-to-warn cases because the ‘significant conflict’ identified by the Supreme Court in *Boyle* is equally present when a federal contract and state tort law differ as to the nature and content of required product warnings.”); *Kerstetter v. Pacific Scientific Corp.*, 210 F.3d 431, 438 (5th Cir. 2000); *Tate v. Boeing Helicopters*, 55 F.3d 1150, 1156 (6th Cir. 1995).
monetary damages or equitable relief, alleging personal injury, death, or property damage arising from the design, manufacture, sale, distribution or use of such certified product or service. The defense applies to products or services sold or distributed to federal, state, or local governments or to private parties. The defense applies regardless of the theory of civil or administrative liability propounded by the claimant. For example, it bars claims sounding in negligence; recklessness; failure to warn; breach of implied warranty; failure to comply with federal, state, or local statute or regulation; indemnity; or contribution.

C. The Defense May Be Rebutted ONLY for Fraud or Willful Misconduct

(1) Fraud or Willful Misconduct

The statute states:

This presumption [that the government contractor defense applies] shall only be overcome by evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the course of the Secretary’s consideration of such technology under this subsection. § 863(d)(1). See also 68 Fed. Reg. at 59691 (same).

The regulations should clarify the circumstances under which the presumption may be rebutted and should impose the burden of rebutting the presumption on the party seeking to overcome it.

The regulations should foreclose any contention that a Seller’s failure to perform additional testing, studies, or analyses of the technology or to detect or warn of potential hazards or limitations constitutes “willful misconduct,” unless there was a knowing and deliberate intent to deceive the Secretary. Proof that the Seller was simply negligent or “reckless” in uncovering additional risks, hazards, or defects, or in failing to warn the Government of such dangers, will be insufficient. Similarly, allegations or proof of the Seller’s failure to perform or recommend additional testing, or to perform or interpret correctly the results of the testing that it did perform or recommend, will not overcome the protection of the defense.

(2) Proof By Clear and Convincing Evidence

A claimant usually must prove fraud by “clear and convincing evidence.” The final regulations should state, therefore, that the presumption that the statutory government contractor

---

2 Under the majority rule, the burden of proof for common-law civil fraud is the “clear and convincing” standard (Addington v. Texas, 441 U.S. 418,424 (1979)). However, some states use a preponderance of the evidence standard and that standard also has been adopted in the civil False Claims Act (31 U.S.C. § 3731(c)).
defense bars any claim relating to the certified technology may be overcome only if a plaintiff proves by clear and convincing evidence that the Seller engaged in deliberately fraudulent misconduct in procuring the certification.

(3) Recommended Amendment

A new subsection is recommended to proposed § 25.6 of the interim rule:

(3) Once the Seller has shown that the Secretary certified the product or service in question as a qualified anti-terrorism technology, a claimant can rebut the presumption that the government contractor defense bars the claim only by proving, by clear and convincing evidence, that the Seller procured the certification by fraud (i.e., that the Seller intentionally made material misrepresentations in its application for the purpose of securing certification on a fraudulent basis) or engaged in similar types of willful misconduct in submitting information seeking approval. The claimant’s burden to show fraud or willful misconduct in connection with the application cannot be satisfied by showing that the Seller (i) knew or should have known about additional hazards associated with the product or service, or (ii) failed to perform additional studies or analyses of the technology that would have detected potential hazards or limitations, or (iii) failed to warn the Secretary about potential hazards or limitations, unless the claimant also establishes there was a knowing and deliberate intent to deceive the Secretary.

D. Clarify Effect of Termination of Designation Resulting from Substantial Modification

(1) Pre-Termination Reliance

The interim rule provides that:

A Designation shall terminate automatically, and have no further force or effect, if the designated Qualified Anti-terrorism Technology is significantly changed or modified. 6 C.F.R. §25.5(i) (68 Fed. Reg. at 59702).

Read literally, the directive to give a designation “no further force or effect” once a certified product or service has been changed significantly could eliminate protection that properly attached before the significant change. For example, the Seller of a product or service using technology certified by the Secretary should continue to enjoy the protection of the certification for that product or service, even if the technology itself is later changed significantly for other products or services. The regulations should state that any loss of protection is not retroactive;
claims arising out of the performance or non-performance of a qualified anti-terrorism technology sold or otherwise conveyed before the designation is terminated will still be subject to all of the SAFETY Act’s provisions. The loss of the designation for the technology should not have any effect on products or services sold or used containing the originally designated and approved technology. Because the SAFETY Act covers all parties in the stream of commerce who rely on the designation and certification, it makes sense that their justifiable reliance not be undermined by retroactive effect back to the time of the change, but rather to the time that the designation is lifted so that they can take reasonable commercial steps consistent with the notice of termination.

In addition, as to products and services that have been certified by the Secretary, the regulations should make clear that where it is the user or purchaser of the certified technology – or any other party other than the Seller itself – who causes a “significant change or modification,” the Seller’s protections under the statute should not be affected.

Finally, the regulations should be clear that the designation cannot be stripped away after the fact by a claimant alleging a significant change, notice of which was not given to DHS. The better course is to revise the interim rule to state that a designation will not be subject to later challenge for the Seller’s failure to give notice.

(2) Recommended Amendment

Proposed § 25.5(i) of the interim rule should be revised to include the following:

The termination of the Designation will apply prospectively and will only affect products or services deployed after the DHS notice of termination. The termination will not affect the rights and protections specified in § 25.6 (relating to the government contractor defense) with respect to any claims relating to products or services sold or otherwise conveyed prior to the termination of the designation by the Secretary. A substantial change or modification to the Qualified Technology without the knowledge and consent of the Seller shall not cause the Designation to terminate, nor shall the Designation be subject to later challenge by third parties for failure of the Seller to give the required notice.
E. Clarify the Application to Anti-terrorism Services

Neither the interim rule nor the commentary address the applicability of the statutory government contractor defense to services as distinguished from tangible products. The interim rule includes services (including support services) in the definition of a qualified anti-terrorism technology (§ 25.3). There is no indication in the interim rule, however, how the statutory government contractor defense will be applied in the certification process to services such as consulting services, design services, software design, and information technology. Many such services are of great potential utility in deterring, preventing, and minimizing the impact of acts of terrorism. As noted in the commentary, the Act provides that during the process of approval for the government contractor defense, the Secretary will conduct a “comprehensive review of the design of such technology and determine whether it will perform as intended, conforms to the Seller’s specifications, and is safe for use as intended.” § 863(d)(2). For example, how would the Secretary apply the above test to a company that supplies training of airport baggage screeners? Services typically do not have a specification or safety testing. There may be a question whether the services alleged to have caused damages are the same ones that were approved. This concern may place a premium on defining the specific services at issue. For this reason, the Secretary should identify a process for review and approval of requests for certification of anti-terrorism services. To reduce uncertainty, the Secretary also might clarify the scope and effect of the government contractor defense as it applies to services.

III. Protection of Intellectual Property and Trade Secrets

DHS’ regulations are not explicit about what protections might or should apply to proprietary information and trade secrets that are included by contractors in their SAFETY Act applications or that result from DHS testing and other evaluation activities. Rather, the regulations merely note that DHS will establish confidentiality protocols and “utilize all appropriate exemptions” from FOIA to protect such confidential information from disclosure.

---

3 The Boyle Court itself indicated that there is no reason to distinguish between products and services. See 487 U.S. at 506 (“The federal interest [in protecting contractors from liability] surely exists as much in procurement contracts as in performance contracts; we see no basis for a distinction.”).


In the preamble to the interim rule, DHS acknowledges the “apprehension” of industry that FOIA does not provide adequate protection.\(^5\) But DHS’s response to such concerns is only to assure industry that DHS “is committed to the protection of applicants’ proprietary information to the fullest extent required or permitted by law.”\(^6\)

The Section believes that the procurement process would benefit from a more proactive approach to protecting the proprietary information and trade secrets of applicants, along the lines discussed more fully below.

**A. General Categories Of Confidential Information**

Three types of confidential information and trade secrets are generally implicated in the SAFETY Act application and review process. DHS should take all of these categories into consideration when addressing this issue in its final rule.

First, contractors’ applications for SAFETY Act coverage of anti-terrorist technologies, as well as associated documentation, likely will contain proprietary information and/or trade secrets that should be treated in a confidential manner by the Government.

Second, anti-terrorist technologies submitted for designation and/or certification under the SAFETY Act are subject (on a case-by-case basis) to scientific study and evaluation by DHS. Relevant areas for consideration include the “effectiveness of the technology,” whether the technology “will perform as intended,” and the appropriate level of third-party insurance given the potential risks to the public and the availability of coverage. The results of such analyses most likely will be derivative of contractors’ proprietary information and/or trade secrets, and therefore should be treated in a confidential manner by the Government.

Finally, where an anti-terrorist technology is designated and/or certified by DHS, the contractor likely will seek confidential treatment of the underlying details surrounding such decision, at least to the extent that they would reveal the contractor’s proprietary information and/or trade secrets. Where DHS rejects an application, however, the contractor may be highly motivated to have the decision itself, in addition to the basis for the decision, treated in a confidential manner by the Government. This is especially true for quasi-commercial technologies that might be sold outside of the anti-terrorist context.

\(^5\) Id. at 59,687 (“Confidentiality of Information” section of preamble). DHS also notes that some commenters on the proposed regulations, which were published on July 11, 2003, 68 Fed. Reg. 41,420, recommended that the regulations include explicit protections and presumptions that would favor the protection of confidential information and trade secrets. Although DHS did not incorporate such recommendations into the Interim Rule, it did not indicate in the preamble to the regulations whether it agreed or disagreed with such recommendations, or explain why.

\(^6\) Id. (emphasis added).
B. Implications of Other Statutory Protections

Exemption 4 under the Freedom of Information Act ("FOIA") prohibits the disclosure of confidential “trade secrets and commercial or financial information obtained from a person.”\(^7\) But the tests crafted by the courts for determining whether information is “confidential” depend, in part, on an initial determination of whether the information was submitted voluntarily. See Critical Mass Energy Project v. Nuclear Regulatory Comm’n, 975 F.2d 871 (D.C. Cir. 1992). Under Critical Mass, information submitted voluntarily will be treated as “confidential,” and protected from release by the Government, if it is the kind of information that the submitter would not ordinarily release to the public.

DHS should make clear that SAFETY Act applications, as well as any resulting analyses, studies, and decisional documentation, are deemed to be “voluntary” submissions, or derivative of such “voluntary” submissions, for purposes of FOIA. By doing so, the regulators will distinguish the SAFETY Act review process from pro-disclosure judicial decisions\(^8\) regarding the compulsory submission of information, such as “cost or pricing data,” under government procurements.\(^9\)

C. Confidential Presumption is Appropriate

DHS should adopt a general presumption of confidential treatment of all SAFETY Act applications, evaluations and studies of such applications, underlying decisional documentation, and application rejection notices. Only application approval notices should be presumed to be disclosable under FOIA.

A potential analogy to the “competition sensitive” approach used in negotiated procurements may be appropriate. See FAR 3.104-3 (prohibitions against disclosing or obtaining procurement information); FAR 3.104-4 (prohibition against disclosure of contractor proposal or source selection information except where specifically authorized, including

---


\(^8\) The Government’s “pro-disclosure” bent under FOIA Exemption 4 was recently highlighted in R&W Flammann v. United States, 339 F.3d 1320 (Fed. Cir. 2003). While addressing a slightly different point (involving information arguably in the public domain as a result of the sealed bid opening process under the FAR), the court made it clear that “FOIA’s broad policy is one of disclosure, as a ‘check against corruption and to hold the governors accountable to the governed.’” Id. at 1323 (quoting NLRB v. Robbins Tire Rubber Company, 437 U.S. 214, 242 (1978)). But this laudable governance objective gives cold comfort to a defense contractor whose “crown jewel” trade secrets are being reviewed by Government officials under the SAFETY Act.

procedures for disputes over confidential designations); FAR 15.207 (“Proposals shall be safeguarded from unauthorized disclosure throughout the source selection process.”).

The downside of this approach is that it results in a rather opaque SAFETY Act application review process. The publicly available body of DHS precedents and rationales would be restricted, affording only limited guidance to future applicants. To mitigate the lack of “sunshine” in the application review process, it would be incumbent upon DHS to regularly publish updated guidelines regarding the general categories of technologies that have been approved and rejected, the generic bases for DHS’s decision-making (without reference to particular technologies or contractors), and the types of backup documentation that contractors should include with their applications to streamline the review by DHS.

Finally, to facilitate meaningful review of DHS denials of SAFETY Act applications, DHS should have in place standard protective order procedures (along the lines of the methods used in procurement bid protests). While protecting the confidentiality of contractors’ intellectual property, this would facilitate the restricted access by non-competitive decision-makers to DHS applications, evaluations, and decisions for the limited purpose of prosecuting such appeals.

D. Impact of Information Sharing on Competitive Procurements

Another concern related to the “coordination” of DHS review with government agency procurements, is the possibility of inadvertent disclosure of the proprietary approaches of competitors, technical transfusion and/or technical leveling that has a direct impact on the procurement. The interim rule makes clear that DHS expects its review to involve substantial back-and-forth between DHS and the Seller/Applicant.

- In the Regulatory History section of the interim rule, at 68 Fed. Reg. 59685, DHS expressly states that the “application process is interactive.”

- Section 25.3(h) permits pre-application consultations in which Sellers may discuss with DHS the need for or advisability of particular types of anti-terrorism technology.

- Section 25.5(c) provides that during the review process, DHS may request additional information from the Seller, or meet with representatives of the Seller.

During this interactive exchange, DHS will be the recipient of substantial quantities of confidential and proprietary information submitted by Applicants; it will have the opportunity (and the obligation) to ask questions about the technologies, to probe the likelihood that they will be successful in reducing the risk of harm, to query the applicability of particular consensus technical standards, to inquire about the nature and extent of testing and analysis, and to clarify issues pertaining to their technical characteristics.
Federal law prohibits government personnel involved in an acquisition from engaging in any conduct that “reveals an offeror’s technical solution, including unique technology, innovative and unique uses of commercial items, or any information that would compromise an offeror’s intellectual property to another offeror.” FAR 15.306(e)(2). In the context of a current procurement, if the same DHS personnel (or the same outside consultants) are using an interactive process to evaluate the technologies of competitors to determine whether they should be designated as QATTs, the opportunity for inadvertent transmission of proprietary information is significant.

DHS has, appropriately, recognized that maintaining the confidentiality of proprietary information obtained from Applicants is a matter of critical importance. The interim rule states, at Section 25.8, that DHS will develop protocols on this issue; the introductory Discussion section of the Federal Register notice states that

All contractors or other agents of the Secretary will be required to enter into nondisclosure agreements, and each will be examined on an Application-by-Application basis for potential conflicts of interest, before being granted access to any confidential information provided by applicants.

68 Fed. Reg. at 59687. This is an important component of protecting proprietary information, but it cannot operate in a vacuum. Contractors or agents of the Secretary may not be aware of all facts and circumstances giving rise to potential conflicts. Applicants also have an obligation to apprise DHS of circumstances that might result in conflicts.

Thus, in order to minimize the risk of inadvertent transmission of proprietary information and/or technical leveling during a review that is “coordinated” with a pending government procurement, the Section recommends that the following provision be included in the regulation:

(1) Applicants whose technologies will or may be used or relied upon in a pending or anticipated government procurement, shall so notify the Department and shall provide the Department with the following information as soon as it is available:

a. The identity of the agency and the contracting office and, if it is available, the solicitation number;

b. Whether the procurement will be competitive, and if not, how the procurement will be conducted;

c. The due date for proposals;

10 In the view of the Section, these requirements should be included in the regulation rather than in unpublished “protocols.” Sellers and Applicants will have more confidence in the protections afforded to their proprietary information if those protections are made a matter of law through promulgation as a formal agency regulation.
d. The anticipated award date.

(2) Upon receipt of such a notice and confirmation with the relevant agency of the time limitations relating to the procurement, the Under Secretary shall expedite consideration of the relevant Application and shall keep both the Applicant and the government agency apprised of its anticipated completion date.

(3) Whenever information provided by more than one Applicant pertains to the same potential or anticipated government procurement, the Department shall

a. Advise each such Applicant that it is evaluating other Applications that pertain to the same procurement; and
b. DHS is not to use the application evaluation process as means to improve the applicant’s technology and under no circumstance should it suggest ideas gleaned from one submission to those making another submission.

(4) Under no circumstances shall evaluators ask for or be provided with a copy of the solicitation, statement of work, or other information identifying the technical requirements of a particular government agency procurement.

(5) In no case shall DHS suggest that changes be made to technologies submitted for any reason but particularly not to improve it, make it more likely to meet requirements in solicitations or to reflect ideas or approaches used by other applicants or technologies.

E. Further Rulemaking is Needed

DHS’s stated policy regarding the protection of contractors’ intellectual property is encouraging, as companies will be more inclined to pursue the SAFETY Act’s statutory protections if they can be assured of confidential treatment by the Government. DHS should consider adding a second policy objective of developing meaningful guidelines based on actual grant and denial precedents to guide future applicants. DHS also should clarify the “voluntary” nature of the SAFETY Act application review process under FOIA. In addition, DHS should consider appropriate measures to protect against the potential misuse of applicant’s information as technical leveling in the procurement process.

The interim rule, however, does not contain any substantive proposals regarding confidentiality and the protection of contractors’ intellectual property. In the absence of a specific proposal by DHS, feedback by industry at this juncture can only be considered “conceptual” in nature. Given the potential complexity in this area, once DHS has reflected upon industry’s comments, it should issue another proposed rule to seek industry’s feedback on
the detailed standards and procedures by which DHS actually intends to protect contractors’ proprietary information and trade secrets.

IV. Determination of Significant Federalism Implications

The Federal Register notice specifically requests comment on the impact of the interim rule with respect to Executive Order 13132 – Federalism. In so doing, the commentary notes that DHS does not believe the interim rule will have a substantial direct effect on the states, on the relationship between the national government the States, or on the distribution of power and responsibilities among the various levels of government. Rather, it notes, States will benefit from this interim rule to the extent they are purchasers of qualified anti-terrorism technologies.

The Section agrees with this assessment, but respectfully adds that the events of September 11, 2001, placed states, localities, and other local units of government (as well as the private sector) at the forefront of the war on terrorism and imposed on them critical national security responsibilities. In administering the SAFETY Act, DHS should consider means to see that the most important technology needs of state and localities that have procurements ready to proceed are addressed as a priority in the designation and certification process under the SAFETY Act.

V. Burdensome Application – Cost Data

On October 17, 2003, DHS also issued its SAFETY Act Application Kit, which contains forms and instructions for Sellers applying for designation and certification of their anti-terrorism technology. The Application Kit had not been previously issued for comment.

The Section is concerned that the extensive cost data required by the application is unnecessary and will, especially given the broad accompanying certification, deter applicants with promising technology. In Sections 12 and 13 of the Application, DHS seeks detailed historical cost data and future cost estimates. The information required includes among other things in Table 12, a detailed breakdown of historical costs for direct materials, direct labor, a complete breakdown of overhead cost components, inventory cost, and profit. Table 13 requires a projection of the future costs in the same categories if the technology is certified as an anti-terrorism technology.

Although the Section appreciates that DHS needs to make a determination under subsection 864(a)(2) of the statute whether the prices or terms of any available insurance will unreasonably distort the sales price of the Seller’s anti-terrorism technologies, it is not clear why DHS requires detailed underlying cost data to make such a determination. Neither the Application Kit nor the interim rule contain any justification or explanation for requiring such information. Nor does DHS indicate what alternatives it might consider.

The submission of such data raises at least two issues. First, contractors and companies with promising technology/services may be unwilling to submit such data – which resembles certified cost or pricing data under the Truth in Negotiations Act (TINA) (10 U.S.C. § 2306a and
41 U.S.C. § 254b). In its most recent amendments to TINA, Congress recognized that the submission of certified cost or pricing data under TINA is a barrier to many technology companies participating in U.S. Government procurements. To address these concerns, Congress and the FAR Council have attempted to alleviate the use of certified data by relying on “Other Than Cost or Pricing Data” (48 C.F.R. 15.403-1) or the Commercial Item Exemption in FAR Part 12. DHS should give consideration to only requiring the minimum amount of information it needs regarding the price (not cost) of the proposed anti-terrorism technology and should revise its application appropriately.

Second, such cost information is extremely sensitive from a competitive standpoint. The points mentioned above concerning protection of such information, both from public release and from unauthorized transfer into a procurement, are equally applicable here.