Congress of the United States
Washington, DC 20515

May 11, 2004

The Honorable Tom Ridge
Office of the Secretary
United States Department of Homeland Security
Washington, DC 20528

Dear Mr. Secretary:

We want to thank you for facilitating the recent meetings between members of our respective Committee staffs and representatives from your office and the Science and Technology Directorate of the Department of Homeland Security (DHS) to discuss progress on the implementation of the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the "SAFETY Act"). It is vitally important that this legislation be implemented as expeditiously and efficiently as possible to ensure that liability concerns do not prevent the development and deployment of anti-terrorism technologies critical to protecting the American homeland.

As you well know, advanced technology companies have many products, services, equipment and devices ready for deployment (and the capability to develop additional technologies) that can detect, deter, or otherwise prevent acts of terrorism – including those involving biological, chemical, radiological, nuclear, and other potentially devastating terrorist weapons and tactics. Unfortunately, these companies have been deterred from making their technologies widely available, and from devoting resources to the development of additional technologies, because of the risk of catastrophic and uninsurable liability that could result from an act of terrorism. Consequently, many anti-terrorism technologies have been deployed only in very limited circumstances by a few entities of the Federal government involved in activities where existing statutory indemnification protections are available.

Congress responded to this problem by passing the SAFETY Act as part of the Homeland Security Act of 2002, P.L. 107-296. The SAFETY Act, now codified at 6 U.S.C. §§ 441-444, sets forth litigation management and liability limitations applicable to persons or entities that sell or otherwise provide anti-terrorism technologies ("Sellers") in an effort to encourage the rapid development and deployment of such products and services. In addition to creating an exclusive Federal cause of action for claims against Sellers arising from an act of terrorism, the statute eliminates liability for punitive damages when terrorists are to blame, limits and apportions recovery of non-economic damages in terrorism cases, and matches the Sellers' total liability following acts of terrorism with the limits of insurance coverage required to be maintained as a condition of SAFETY Act designation.

As the statute itself suggests, the analysis to be undertaken by the Department for the

PRINTED ON RECYCLED PAPER

designation and certification of a given technology was intended to be simple and straightforward – a means of *facilitating* transactions, *not* erecting additional barriers to deployment. The Department's limited role, in the first instance, is to conduct a basic analysis of the technology to confirm that it actually works and would not pose an inherent risk of injury to others. Once that threshold is passed, the Department should use input from the insurance marketplace and pricing information provided by the applicant to develop an optimal liability limit and level of insurance coverage that Sellers must maintain that will not unreasonably distort the selling price of the technology.

In order to ensure the overall success of this program, it is vitally important that SAFETY Act review be seen as an efficient gateway to commercially-advantageous and air-tight protections for Sellers (and other contractors, subcontractors, suppliers, and vendors to the extent of their involvement in the manufacture, sale, use, or operation of the technology) from liability for acts of terrorism, not an uncertain process in which critical homeland security devices and services can get bogged down in lengthy and burdensome bureaucratic reviews. Unfortunately, we are concerned that the latter scenario may be the one that is unfolding. To date, we understand that DHS has received disappointingly few SAFETY Act applications, and has yet to designate a single technology – even though some applications have been pending since late last fall.

Indications from leaders in the anti-terrorism technology industry suggest that the application process itself and questions about the efficacy of the liability protection may be to blame for the delay, and for the reluctance of many companies to seek the protections of the SAFETY Act. We have reviewed the Interim Rule and the application kit currently in use and find that there are, indeed, a number of problems that can and should be swiftly addressed. Many of the concerns about the application kit were communicated in the meeting among our respective staffs and, to your credit, the SAFETY Act implementation office within the Science and Technology Directorate has indicated a willingness to reconsider and revise the application process.

Included below, for your information and attention, is a discussion of our major concerns with respect to DHS implementation of the SAFETY Act.

First, we want to **unequivocally dispel any lingering notion that the SAFETY Act is to be narrowly construed and applied**, or is somehow intended to address only those limited situations in which a technology would not otherwise be insurable. The manifest intent of the SAFETY Act is to encourage the broadest possible deployment of technologies that make America safer. Even Sellers who have been able to obtain some level of insurance to cover liabilities associated with their anti-terrorism technologies may be dissuaded or prevented by high terrorism insurance costs and other terrorism risk management considerations from obtaining the additional coverage necessary for deploying their technologies as widely as possible. SAFETY Act liability protections should be extended to those Sellers who may be able to obtain some limited insurance coverage, but whose overall potential exposure to liability for acts of terrorism prevents them from cost-effectively obtaining additional insurance that would allow broader deployment of their anti-terrorism technology.

Second, we believe it is absolutely **essential that the Department initiate a process to prioritize applications for SAFETY Act designation and certification, and ensure that critical technologies receive expedited treatment**. Although the Interim Rule suggests that you anticipate expedited review for certain technologies, we are not aware that any formal procedures have been established. We would expect that under any formal prioritization:

- Promising anti-terrorism technologies responsibly designed to prevent or respond to the gravest terrorist threats – as determined by the Department's Information Analysis and Infrastructure Protection Directorate – would receive preferential and expedited review.
- Technologies awaiting designation or certification that are the subject of important procurements involving DHS or other government agencies or entities that bear critical, front-line homeland security responsibilities would receive priority treatment.
- Pending applications that may have critical deployment possibilities during a time of heightened risk or relating to a current terrorism alert may warrant expedited review or special approval of the Secretary. We cannot allow a circumstance in which DHS is warning of a particular type of attack while at the same failing to expedite deployment of potentially preventive technologies.
- In the case of technologies with which a government agency already has had substantial experience, or for which it has data demonstrating effectiveness – either through the procurement process or through prior use – the Department should defer to the judgment of the procuring agency on the effectiveness of the technology and thereby expedite its review.

It is also important that **DHS not view the SAFETY Act application process as requiring the Department to insert itself in a pending transaction for the purpose of establishing performance standards** for a given technology. The statute provides no such authority. If, for example, a city government and an anti-terrorism technology manufacturer have negotiated a contract to purchase biohazard detectors, and have made consummation of the deal contingent upon SAFETY Act designation and certification of the biohazard detectors, the Department's review should not involve a *de novo* determination of whether the detectors meet a particular performance standard. Rather, the SAFETY Act's emphasis on availability for "immediate deployment" and on an assessment of "risk exposure to the public if such anti-terrorism technology is *not* deployed" (emphasis added) requires that DHS rely to the maximum extent possible on the purchase contract itself as evidence of "substantial utility and effectiveness." 6 U.S.C. § 441(b). The statute states that prior U.S. Government use presumptively establishes "substantial utility and effectiveness." Likewise, strong deference should be given to State and local governments having experience with such products. Unless the design or operation of the product itself poses inherent risks to the public, the technology should be promptly designated or certified.

Additionally, **where pending procurements are involved, the Department should defer to the judgment of the buyer and utilize information already provided in connection with the procurement**, rather than reconstruct a process the parties already have diligently undertaken. The due diligence of a prospective buyer in the course of a procurement will ordinarily have addressed many of the statutory criteria for designation, including:

- Prior United States Government use or demonstrated substantial utility or effectiveness. 6 U.S.C. §441(b)(1).
- Availability of the technology for immediate deployment in public and private settings. 6 U.S.C. §441(b)(2).
- Magnitude of risk exposure to the public if such anti-terrorism technology is not deployed. 6 U.S.C. §441(b)(5).
- 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. 6 U.S.C. §441(b)(6).
- 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. 6 U.S.C. §441(b)(7).

Other SAFETY Act criteria may also be partially addressed through the procurement process, and require only modest additional input for the Department's review. Utilizing this information and according appropriate deference to the judgment of the buyer should expedite the process and help achieve the statutory goal of "immediate" deployment of protective technologies.

We are also **concerned about the Department's apparent intent to condition designation and certification of anti-terrorism technologies on the Seller satisfying additional operating criteria**. The value of SAFETY Act protections to Sellers is completely dependent on whether the liability limitations will actually apply to prevent them (and others in the supply chain as contemplated in the statute) from incurring the kind of staggering liability that has thus far prevented widespread development and deployment of critical technologies. Attaching conditions to designations or certifications could create the kind of litigation loophole that would defeat the entire purpose of the SAFETY Act. This is an unacceptable result. In order to fulfill the purposes of the SAFETY Act, **designations and certifications should, to the greatest extent practicable, explicitly and unconditionally cover the operation of the anti-terrorism technology** and all elements of the development, sale and acceptance of the product or service, including any written materials, instructions or warnings; any training, installation, maintenance, and repair; and any other components, services and relevant intangibles provided by the Seller.

DHS also should **revisit the "change or modification" provision** of the Interim Rule 25.5(i), which states that SAFETY Act protections will terminate automatically if the technology is changed in a manner that "could significantly reduce the safety or effectiveness of the technology." This, too, creates a conditional designation, and opens a litigation loophole that is directly contrary to the statutory intent. This provision must be refined and tightened to ensure certainty with respect to the liability protections contemplated in the SAFETY Act.

Finally, **the application process associated with SAFETY Act designation and certification must be tailored in a way that is as efficient, streamlined and secure as possible.** The current iteration of the application kit, which we understand to be in the process of substantial revision, must be simplified in the following ways to require only the volume and kind of information absolutely necessary to satisfy the Department's due diligence requirements and the statutory goal of "immediate" deployment:

- **Requests for speculative assessments of unquantifiable terrorism-related risks should be eliminated.** By way of example, Application Item 3, which requires the applicant to set forth "envisioned threat scenarios"; Application Form Item 12a, which requests the "estimated potential magnitude of harm to the public" for "Typical Case" and "High-Loss Case" scenarios broken down by fatalities, injuries, economic losses, physical damage, mass disruption, and symbolic damage; and Application Form Item 13, which requests information on "psychological impacts that might well arise," all request unnecessary and speculative information. The Department is in the best position to make these kinds of assessments – particularly with respect to terrorist threats – and the applicant should not be required to certify such hypothetical information.

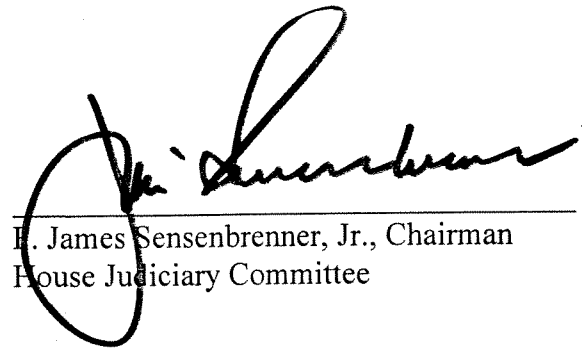
- **Requests for business and financial information should be kept to a minimum.** The statutory test of whether "extraordinarily large" or "unquantifiable" risk exposure exists for the Seller is not dependent on the financial condition of such persons. Moreover, the statutory test of whether a "substantial likelihood" of non-deployment of the technology exists will be satisfied in most cases where immediately deployable technologies having willing purchasers are nonetheless not being sold in the marketplace.

  In the exceptional case where it is appropriate or necessary to request business or financial information, such data should be accepted in a format widely utilized for cost-accounting purposes. We note particularly that large amounts of financial data and other proprietary business information will ordinarily be unnecessary for determination of the maximum amount of insurance coverage that will not unreasonably distort the selling price of the technology. Such determinations should be made to the greatest extent possible on the basis of insurance market data, and projected usage of the technology. Additionally, the Department should institute strong confidentiality protocols for maintaining proprietary information, and include such protocols in any Final Rule.

- **Requests for insurance-related information should be aimed primarily at securing marketplace driven estimates** of the costs associated with providing coverage for a given technology. Absent a compelling basis for requesting the information, Designation Application Item C.11 should be modified to eliminate requirements for historical insurance information, and information on insurance maintained by the Seller that is unrelated to the anti-terrorism technology at issue.

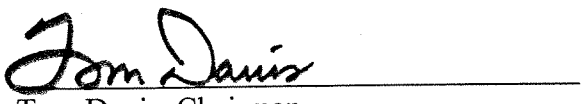
We look forward to continued cooperation with the Department on this urgent matter. We look forward to your efforts to address all of these issues, and to ensure the successful implementation of the SAFETY Act application process. In the interest of protecting the American people from the threat of global terrorism, we must work together to see that liability protections are put in place to encourage the wide deployment of critical anti-terrorism technologies. We trust you will give these concerns your immediate attention and would request a formal response within the next two weeks.

Sincerely,



F. James Sensenbrenner, Jr., Chairman
House Judiciary Committee

Christopher Cox, Chairman
Select Committee on Homeland Security



Tom Davis, Chairman
House Committee on Government Reform

cc: Hon. J. Dennis Hastert, Speaker
Hon. John Conyers, Jr., Ranking Member
House Judiciary Committee
Hon. Jim Turner, Ranking Member
House Select Committee on Homeland Security
Hon. Henry A. Waxman, Ranking Member
House Committee on Government Reform