

## Alert

### **HOMELAND SECURITY ACT LIMITS VENDOR LIABILITY AND MAY PROVIDE MARKETING BOOST**

The Homeland Security Act of 2002, which provides for a major restructuring of the organization of the executive branch of the United States government, will also enable Sellers (as defined in the Act) and providers of qualified anti-terrorism technologies to limit their liability in cases of terrorism. In addition, providers of such technologies might get a marketing boost by being certified in accordance with the Act.

Congress, believing that important technological innovations that could be used in the defense against terrorism might be kept from the marketplace because of liability fears, passed the "Support Anti-terrorism by Fostering Effective Technologies Act of 2002," also known as the "Safety Act," as part of the Homeland Security Act (§§ 861-865). The Safety Act provides limitations of liability for providers of "qualified anti-terrorism technology." The Secretary of the Department of Homeland Security will determine which technologies qualify for the liability limitations under the system of risk management provided for in the Act.

Such technology is very broadly defined as "any product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause." (§ 865(1)). The Act provides certain criteria that shall be used in determining qualified technology, which "shall" include:

Prior United States Government use or demonstrated substantial utility and effectiveness.

Availability of the technology for immediate deployment in public and private settings.

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.

Copyright ©2003 by Kaye Scholer LLP. All Rights Reserved. This publication is intended as a general guide only. It does not contain a general legal analysis or constitute an opinion of Kaye Scholer LLP or any member of the Firm on the legal issues described. It is recommended that readers not rely on this general guide in structuring individual transactions but that professional advice be sought in connection with individual transactions. References herein to "Kaye Scholer LLP & Affiliates," "Kaye Scholer," "Kaye Scholer LLP," "the Firm" and terms of similar import refer to Kaye Scholer LLP and its affiliates operating in various jurisdictions.

JANUARY 2003

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.

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. (§862(b)).

The Act provides for a Federal cause of action for claims that result or may result in loss to a Seller of such technology arising from terrorism (as defined in the Act) when "qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act." (§863(a)(1)). The Federal cause of action applies to sales to both "Federal and non-Federal government customers."

The Act prohibits punitive damages and limits noneconomic damages. Noneconomic damages may only be awarded against a defendant in an amount directly proportional to the percentage of responsibility of the defendant, and a plaintiff may not recover noneconomic damages unless the plaintiff suffered physical harm. Also, any recovery by a plaintiff shall be reduced by any compensation the plaintiff receives or is entitled to receive from collateral sources. The Act also provides a rebuttable presumption that the government contractor defense applies, even for sales of product to non-Federal government customers.

The Act provides that the Secretary of Homeland Security shall review the design of the anti-terrorism technology, determine whether it will perform as intended, whether it conforms to the Seller's specifications and is safe for use as intended. After review and approval, the Secretary will issue a "certificate of conformance" and place the technology on an "Approved Product List for Homeland Security." (§ 863(d)(3)). Whether or not intended as such by Congress, this certificate and listing could potentially be a good marketing tool for vendors.

The Seller must also obtain liability insurance in amounts and types as specified by the Secretary. The amount of such insurance need not be "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." (§ 864(a)(2)). The Act caps a Seller's liability (including for indemnification claims) by the amount of the liability limits of the required insurance.

The Act also provides for a reciprocal waiver of claims and requires Sellers to enter into a "reciprocal waiver of claims with its contractors, subcontractors, suppliers, vendors and customers, and contractors and subcontractors of the customers." The waiver shall require each party to be responsible for its losses (including those of its employees) resulting from an act of terrorism when qualified anti-terrorism technologies have been used. (§ 864(b)).