SAFETY Act Liability Protections for Air Cargo Screeners

By Alice Crowe

In August 2007, Congress enacted the Implementing the Recommendations of the 9/11 Commission Act of 2007 (the 9/11 Act),1 which requires the Transportation Security Administration (TSA) to establish a system for screening all cargo transported on passenger aircraft within three years.2 In response, the TSA developed the Certified Cargo Screening Program (CCSP), under which the TSA may certify entities in the cargo supply chain to screen cargo for unauthorized explosives at off-airport facilities.3 Some entities certified as Certified Cargo Screening Facilities (CCSFs) screen cargo by physical search, while others use technology approved by the TSA, such as X-rays or explosive trace detection devices. The Department of Homeland Security (DHS) may designate CCSP screening measures as qualified antiterrorism technology (QATT) under the Support Antiterrorism by Fostering Effective Technologies Act (the SAFETY Act).4 Once the DHS designates or certifies a technology, the seller of the technology enjoys certain liability protections under the SAFETY Act.

This article describes the key cargo screening provisions of, and policies underpinning, the 9/11 Act and the SAFETY Act as well as the domestic programs the DHS and TSA have established thereunder. The discussion also considers whether a CCSF that fails to detect an explosive in cargo because of human error or negligence nonetheless may benefit from the SAFETY Act’s limits on liability. The article concludes that it is unlikely that human error would vitiate those liability protections. A CCSF that is negligent in its implementation of a designated QATT, however, may jeopardize its statutory protections from liability if its performance of cargo screening departs significantly from the specific methodology that provided the basis for its designation or certification by the DHS.

The 9/11 Act’s “100 Percent Screening” Mandate

The Transportation Security Administration has implemented a multilayered, risk-based system for securing cargo transported on passenger aircraft.5 Approximately 10 million pounds of cargo are transported on passenger aircraft in the United States each day. U.S. aircraft operators and foreign air carriers operating at U.S. airports must ensure that cargo transported on passenger aircraft is screened as set forth in their TSA-approved security programs.6 Prior to the 9/11 Act, aircraft operators screened most cargo at the airport.7

The 9/11 Act requires that the system used to screen cargo provide a level of security “commensurate with the level of security for the screening of passenger checked baggage” and directed that 100 percent of such cargo be screened not later than Aug. 3, 2010.8 The act defines “screening” as “a physical examination or non-intrusive method of assessing whether cargo poses a threat to transportation security. Methods include X-ray systems, explosive detection systems, explosive trace detection devices, explosive detection canine teams certified by the TSA or a physical search together with manifest verification.”9

On Sept. 16, 2009, the TSA issued an Interim Final Rule establishing regulations to implement the statutory mandate to screen all cargo on passenger aircraft by Aug. 3, 2010.10 This rule applies only to cargo loaded in the United States and not to cargo loaded abroad and transported into the United States.11 The TSA’s objective was to develop a domestic program that could achieve “100 percent screening,” while still allowing commerce to flow.12 The agency concluded that the “100 percent screening” mandated by the 9/11 Act could not be achieved by relying solely on U.S. aircraft operators and foreign air carriers to conduct screening.13 Under the CCSP, facilities upstream in the air cargo supply chain—such as shippers, manufacturers, warehousing entities, distributors, third-party logistics companies, indirect air carriers, and independent cargo screening facilities—may apply to become a TSA-certified facility and screen cargo off-airport.14 A CCSF applicant must successfully undergo a TSA-conducted security threat assessment15 and submit to an evaluation of its facility by the TSA.16 Once certified, a CCSF must take the following measures:

- implement a TSA-approved standard security program;17
• ensure that key personnel with unescorted access to cargo undergo the required security threat assessment;48
• adhere to strict physical and access control measures for the storage, handling, and screening of cargo; and
• implement chain-of-custody measures to ensure the security of cargo as it moves through the supply chain, from the time of screening until loading onto passenger aircraft.19

The SAFETY Act
Congress passed the SAFETY Act in response to the terrorist attacks of Sept. 11, 2001. Realizing that “technological innovation is the Nation’s frontline defense against the terrorist threat,”20 Congress intended the SAFETY Act to serve as a catalyst for private businesses to develop and market systems, devices, and services that could be used to combat terrorism.21 Congress recognized, however, that exposure to liability could inhibit companies from bringing such new technologies to market. This risk is inherent because an antiterrorism technology or integrated system of technologies may be defeated even if it is operated as designed. The SAFETY Act provides “a narrow set of liability protections for manufacturers of these important technologies.”22 To receive these protections from liability arising from acts of terrorism at a site using an antiterrorism technology, firms that manufacture or provide such technology must apply to the DHS for either “designation”23 or “certification”24 of the technology as a QATT.

“Designation” and “Certification” Protection
Technologies for which the DHS may extend SAFETY Act’s liability protections include “products, equipment, services (including support services), devices and other 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.”25 Both products and services are eligible to receive the same level of liability protection under the SAFETY Act. If, after a technical review, the DHS “designates” the technology as a QATT, the following protections apply to the seller:26

• exclusive jurisdiction in federal courts for claims based on an “act of terrorism”27 associated with deployment of a QATT;28
• liability capped at an amount no greater than the limits of liability insurance that the DHS requires the seller to maintain as a condition of designation or certification;29
• limitation on liability for noneconomic damages in proportion to the seller’s responsibility and only if the plaintiff has suffered physical harm;30
• a complete bar on punitive damages or prejudgment interest;31 and
• reduction of the plaintiff’s recovery by the amount of any collateral source compensation, such as insurance benefits or government benefits.32

The SAFETY Act’s limited liability protections extend to users and component providers of the technology through-out the supply chain, both downstream and upstream.33

The SAFETY Act provides that, before issuing a certification for a technology, the DHS will conduct a “comprehensive review of the design of such technology, and determine whether it will perform as intended, conforms to the Seller’s specification, and is safe for use as intended.”74 A seller who qualifies for this DHS certification receives all of the above protections provided by “designation” as well as the added protection of a rebuttable presumption that a statutorily created “government contractor defense” applies to the certified QATT.35 The government contractor defense is an affirmative defense that immunizes sellers from liability for claims “arising out of, or relating to, or resulting from an Act of Terrorism (as defined by the SAFETY Act) when QATTs have been deployed, and such claims result or may result in loss to the Seller.”36 Certification entitles the seller to a presumption that such claims will be dismissed immediately.37 This presumption can be overcome only by evidence showing that the seller acted fraudulently or with willful misconduct when submitting information to the DHS during the certification review process.38 The government contractor defense is available not only to government contractors but also to those who sell to state and local governments or the private sector.39

Once a technology has been certified, the DHS issues a certificate of conformance to the seller, and the technology is placed on the department’s published Approved Products List.40 The DHS has issued significantly fewer certifications than designations.41 Through July 2010, a total of 175 SAFETY Act applications were filed and 57 SAFETY Act awards were approved, only nine of which were certifications.42 To date, all the approved SAFETY Act applications for CCSFs have been for designation only; none has received certification.

A certified cargo screening facility is eligible for designation as a qualified antiterrorism technology under the CCSP. A CCSF that conducts screening by X-ray, an explosive trace detection device, or a physical search may be a “seller” of that technology under the SAFETY Act. Once the TSA certifies a CCSF to screen cargo, the facility may apply for SAFETY Act protection.43 As part of its review, the DHS evaluates a CCSF’s economic background, which includes financial information and risk exposure, and determines the liability cap for that facility. CCSFs may choose to obtain liability insurance equal to the liability cap or to self-insure. As long as the CCSF uses the QATT as described in the designation, that CCSF will receive the protections afforded by its designation under the SAFETY Act.44

Do the SAFETY Act’s Liability Protections Extend to Aircraft Operators?
It is unclear whether an aircraft operator that accepts CCSF-screened cargo would be protected by the limitations on liability under the CCSP’s designation. As noted, the act creates an exclusive federal cause of action “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 antiterrorism technologies have been deployed in defense against or response to recovery from such act and such claims result or may result in loss to the Seller.”45
exclusive “Federal cause of action shall be brought only for claims for injuries that are proximately caused by Sellers that provide qualified antiterrorism technology.” The DHS’s interpretation of the SAFETY Act is that (1) only one cause of action exists for loss of property, personal injury, or death for performance or nonperformance of the seller’s QATT in relation to an act of terrorism, and (2) such cause of action may be brought only against the seller of the QATT and may not be brought against the buyers, the buyers’ contractors, downstream users of the QATT, the seller’s suppliers or contractors, or any other person or entity. Therefore, under this interpretation, an aircraft operator, as a downstream customer of the CCSF, would receive the protections of the SAFETY Act for claims relating to and within the scope of coverage of the CCSF’s designation. Because not all claims may be deemed to be within the scope of SAFETY Act designation, aircraft operators should consider obtaining additional protection, depending on their risk tolerance. In addition, an aircraft operator may apply for a separate designation for the screening processes it performs—that is, verification that the chain of custody is still intact prior to loading the cargo on passenger aircraft and rescreening of the cargo if the cargo shows signs of tampering. These important security functions may be independently eligible for designation under the SAFETY Act as a QATT.

Can Human Error or Negligence Defeat the SAFETY Act’s Protections?

It is axiomatic that no screening technology can prevent, mitigate, or respond to all types of terrorist acts and that sellers of technologies are likely to be subject to third-party liability claims if an act of terrorism occurs. The SAFETY Act envisions the judicial system as the enforcement mechanism for SAFETY Act awards if an act of terrorism occurs and third-party lawsuits against sellers of QATTs ensue. In hearing a third-party lawsuit, it is likely that a court, in addition to considering the specific facts of a case, would analyze whether the seller used the QATT in accordance with the terms of its SAFETY Act designation or certification. Because the Certified Cargo Screening Program is relatively new, courts have not yet adjudicated when a technology is “outside the scope of a designation or certification.” These will be among the most important questions courts will face when determining whether SAFETY Act protections apply, especially if a deviation in the technology—including any incidents related to human error or negligence—has occurred. Depending on the facts of a particular case, a court could find that the SAFETY Act’s protections apply even in the event of human error or negligence. The DHS’s SAFETY Act awards cover QATTs that are “within the scope,” meaning they are consistent with the award language in the description of the technology the DHS attaches as Exhibit A to its designation or certification documentation. To ensure that sellers have fair notice of the scope of SAFETY Act coverage, an Exhibit A technology description is made as precise as possible. A seller is required to notify the DHS if it makes (or intends to make) changes that cause the QATT to be outside the scope—that is, not as described in Exhibit A to its designation or certification. Modifications that do not cause the QATT to be outside the scope of its Exhibit A description will not adversely affect coverage and they do not require that the DHS be notified of the change.

It is the seller’s obligation to ensure that any modification remains within the scope of its designation or certification. The seller bears the risk that SAFETY Act protections might not apply if a court were to rule that a deviation to the technology was outside the scope of the SAFETY Act award. Therefore, notice to the DHS of a potential modification is always a sound precaution for sellers. Moreover, as part of the technical evaluation, the DHS considers whether normal error rates for a technology would allow it to be considered “effective,” in accordance with the DHS’s criteria for designation and certification. Those criteria tolerate (and may even assume) a certain degree of potential error in the operation of the technology. The DHS examines how the seller mitigates the potential for human error by evaluating the seller’s training materials, quality assurance mechanisms, quality control audits, and best practices guidance and instructions.

Can Human Error or Negligence Defeat the SAFETY Act’s Protections for CCSFs?

Assuming that a CCSF designation is valid, to what extent could human error or negligence place a QATT outside the scope of the SAFETY Act’s liability protections? Would a CCSF forfeit its SAFETY Act protections if it had implemented all processes of the designated QATT but employed a screener who had failed to detect an explosive device displayed on an X-ray monitor? Would it matter whether the failure to detect the device was caused by human error or negligence? Again, the answer may depend on whether the screening actually carried out is within the scope of the designated QATT or whether, through human error or negligence, results in a “significant modification” in practice that renders the technology outside the scope of the QATT. For example, in a situation in which the CCSF complies with all the requirements of the designated QATT, maintains the equipment according to the manufacturer’s instructions, trains the screener properly, and applies quality control measures, but the screener still fails to detect the explosive, a court could consider the QATT within the scope of its SAFETY Act award. In this scenario, the failure to detect the explosive device is based on human error and not on an actual modification that reduced the effectiveness of the technology. If the mistake was isolated and not part of a larger pattern of systemic negligence, a court could find that the CCSF would still be entitled to the SAFETY Act’s limitations on liability. In contrast, if the CCSF is negligent, fails to use proper screening protocols, does not maintain the equipment properly, and fails to train employees and implement quality controls, thereby reducing the effectiveness of the designated technology, the seller may bear the risk of losing SAFETY Act protections.

Conclusion

Technological innovation is the nation’s first line of defense against terrorism. The U.S. Congress passed the SAFETY Act to serve as a catalyst for businesses to develop systems to
combat terrorism. Congress recognized, however, that industry’s fear of potential exposure to liability is likely to retard the development and deployment of effective antiterrorism technologies. As a result, Congress included provisions in the SAFETY Act that would limit the liability of sellers of such technology if a terrorist incident occurs. Through the Certified Cargo Screening Program, the Department of Homeland Security has established a mechanism that may enable sellers of technologies to qualify for the SAFETY Act’s liability protections, thus removing a potential significant barrier to the development of effective systems to combat terrorism. Ultimately, however, it is the courts that will determine the effectiveness of the SAFETY Act as they interpret the scope and applicability of the liability protection provided by the act, particularly in cases where human error or negligence contributes to a screening failure. One would hope for security’s sake that the courts’ decisions will not inhibit companies from bringing new technologies to market. TFL

Alice Crowe is senior counsel at the Department of Homeland Security’s Transportation Security Administration. The views reflected in this article are those of the author and do not represent the position of the TSA or the DHS. The author is grateful to Francine Kerner, Denise Starr, Allison Jetton, Nicole Marcson, Bruce Davidson, Aida Stark, Ross Dembling, and Mardi Thompson for their valuable advice and assistance. This article was previously published in Volume 23, No. 4 of The Air & Space Lawyer, published by the American Bar Association Forum on Air and Space Law.

Endnotes


2Section 1602 of the 9/11 Act added 49 U.S.C. § 44901(g) (1) to require 100 percent screening (“[n]ot later than 3 years after the date of enactment of the 9/11 Act, the Secretary of Homeland Security shall establish a system to screen 100 percent of cargo transported on passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation to ensure the security of all such passenger aircraft carrying cargo.”).


749 C.F.R. § 1549.101(d). The CCSP allows entities to screen cargo before it is consolidated. The CCSP includes a Screening Technology Pilot Program for evaluating the effectiveness of cargo screening technology such as X-rays or electronic trace detection devices. The TSA will continue to evaluate technologies that allow for bulk screening of some types of consolidated cargo to eliminate the need to break down such cargo and screen it piece by piece. This search for technological advancement is an integral part of the CCSP.


10H.R. Rep. No. 107-6091 at 1399 (2002). See also Regulations Implementing the Support Antiterrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act), 71 Fed. Reg. 33147, 33148 (June 8, 2006) (to be codified at 6 C.F.R. pt. 25) (the purpose of the act “is to ensure that the threat of liability does not deter potential manufacturers or sellers of antiterrorism technologies from developing, deploying, and commercializing technologies that could save lives”).


14The DHS could also issue a Developmental Testing and Evaluation Designation for technologies that could serve as homeland security resources but require additional testing and evaluation. Such a designation would provide SAFETY Act liability protection for a limited term not longer than 36 months and usually limited to certain deployment sites. 6 C.F.R. § 25.4(f).

15Section 25.2 of the DHS regulations defines an “act of terrorism” as “…any act determined to have met the following requirements … :

16(1) Is unlawful;

17(2) Causes harm, including financial 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

SAFETY ACT continued on page 45
SAFETY ACT continued from page 27

(5) Uses or attempt 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.

6 C.F.R. § 25.2; see also 6 U.S.C. § 444.

The DHS defines noneconomic damages to mean damages for losses resulting from 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. 6 C.F.R. § 25.2.


Id. § 443(c).

The DHS has stated that “[w]hile certain proposed significant modifications should require review, many routine or non-significant modifications will not.” 71 Fed. Reg. 33153 (June 8, 2006). The DHS elaborated: “When a Seller makes routine changes or modifications to a QATT such that the QATT remains within the scope of the description set forth in the applicable Designation or Certification, the Seller shall not be required to provide notice to the DHS, and the changes or modifications shall not adversely affect the force or effect of the Sellers QATT Designation or Certification.” 6 C.F.R. § 25.6(d) (emphasis added).


On Aug. 31, 2010, the DHS issued a Block Designation for CCSFs, see www.safetyact.gov.

35Id. § 442(a)(1).

6 C.F.R. § 25.6(d)(2).

This outcome would be consistent with laws that regulate general liability insurance, for which coverage is provided for “occurrence” defined as “an accident, including a continuous or repeated exposure to conditions, which results in bodily injury or property damage neither expected nor intended from the standpoint of the insured.” COUCH ON INSURANCE (5th ed. 2010), § 126:29. Thus, a mistake or unintentional negligence would be considered an “occurrence” and covered by insurance. Public policy compels refusal of coverage for intentional actions. Farm-land Mut. Ins. Co. v. Scruggs, 886 So. 2d 714, 721 (Miss. 2004).