## Table of Contents

I. What does a SAFETY Act designation mean to ACC member companies and Responsible Care Partners? .......................................................... 3

II. What constitutes a terrorist attack for SAFETY Act purposes? ......................... 4

III. What does an ACC member company or Responsible Care® Partner need to do to receive SAFETY Act protection? .......................................................... 4

IV. What can ACC member companies and Responsible Care Partners do to maximize the likelihood that the designation will limit their individual liability? ..... 5

V. What should a ACC member company do if they want more information?........ 6

VI. Frequently Asked Questions............................................................................. 7
The Responsible Care® Security Code and the SAFETY Act: A Valuable Liability Management Tool

The Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (“SAFETY Act” or “Act”) authorizes the U.S. Department of Homeland Security (“DHS” or “Department”) to designate certain anti-terrorism products or services as “qualified anti-terrorism technologies” (“QATT”) and thereby limit the potential liability of private entities who employ them to mitigate the risk of a terrorist attack.

The Department recently granted the American Chemistry Council (“ACC”) a SAFETY Act Designation (“Designation”) for its Responsible Care Security Code (“Code” or “RCSC”).

I. What does a SAFETY Act designation mean to ACC member companies and Responsible Care Partners?

The designation of the RCSC as a QATT provides ACC member and Responsible Care Partner companies that have implemented the Code and the Responsible Care Management System® a potential reduction in liability associated with terrorist threats.

If the Department grants an anti-terrorism product or service a Designation as a QATT, a plaintiff alleging a deficiency relating to that QATT in a suit following a terrorist attack may only sue the “seller” and not the customer or user of that QATT; may only sue in federal court; and may only recover up to the amount covered by the insurance carried by the seller and approved by the Department for that QATT. In addition, the seller cannot be liable for punitive damages; cannot be jointly and severally liable for “noneconomic damages”; and cannot be liable for noneconomic damages at all, absent physical injury.

ACC is the “seller” of the QATT, as it provides the RCSC to ACC member and Responsible Care Partner companies and requires implementation of the Code as a condition of membership or Partnership. The ACC member and Responsible Care Partner companies, which are required to adopt and implement the RCSC as a condition of membership or partnership, qualify as “customers” or “downstream users” of the RCSC and, thus, can be covered by the SAFETY Act’s liability limitations. The Department has concluded that such customers or users are protected from suit, as only the seller (ACC) is a proper defendant.

ACC’s liability stemming from the Code in the wake of an act of terrorism is subject to SAFETY Act limitations and is limited to the amount of insurance required in the Designation ($9,000,000 per occurrence).
Although the Designation is a potentially important tool for limiting liability following a terrorist attack, no court has ever construed the SAFETY Act or the regulations implementing it, so the full scope of liability relief available from the Designation is not yet certain.

II. What constitutes a terrorist attack for SAFETY Act purposes?

A terrorist attack is any act that is:

- Unlawful
- Causes harm to a person, property or entity in the United States, and
- Uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.

III. What does an ACC member company or Responsible Care® Partner need to do to receive SAFETY Act protection?

The Designation’s description of the RCSC defines the set of practices that comprise the technology and, in turn, the scope of liability protection under the Act. The Act’s liability protection can extend only as far as the QATT is implemented, as described in the Designation.

The description of the RCSC in the Designation includes three principal components:

- The QATT provides a “management framework that is designed to identify, assess, and address vulnerabilities, prevent or mitigate incidents, enhance training, and increase response capabilities” in order to “respond to a physical or cyber attack against any form of chemical operation, whether at a fixed facility or during transportation.”

- The QATT directs member and Responsible Care® Partner companies to implement the security framework, consisting of 13 particular management practices (in the RCSC), and identifies particular documents to guide the implementation (e.g., Site Security Guidance, Value Chain Guidance, Cyber Security Guidance, RCMS® Technical Specification, etc.). Implementation in conformity with these guidance documents constitutes presumptive compliance with the Code, though not the exclusive means of compliance.
• The QATT provides for oversight of implementation by ACC member and Responsible Care® Partner companies through progress reports to ACC, periodic certification by independent third parties, and application of ACC’s governance procedures.

This broad definition benefits ACC member and Responsible Care Partner companies implementing the technology because it provides potential SAFETY Act coverage for activities within the scope of the Designation.

IV. What can ACC member companies and Responsible Care Partners do to maximize the likelihood that the designation will limit their individual liability?

*If a terrorist attack occurs, the extent of protection afforded by Designation could depend on the ability of the ACC member or Responsible Care Partner company to identify not only that the Code has, in fact, been implemented—as embodied in the management practices, guidance documents, and oversight procedures specified in the Designation—but also that any challenged actions (or inactions) fall within the scope of the implementation.*

In order to maximize the potential that the Designation applies to the broadest range of potential allegations, ACC member and Responsible Care Partner companies should ensure that their recordkeeping systems explicitly identify and document how even facility-specific security measures flow from and are part of their implementation of the RCSC. The following are our initial and general recommendations for accomplishing this goal.

1. Companies implementing the Code should ensure that their current recordkeeping system identifies the measures taken by the company in implementing the Code as a QATT under the SAFETY Act. Such documentation should cover actions at every appropriate organizational level—from management down to specific facilities— including, for example, everything from high-level security assessments to site-specific security measures to training exercises. To the extent that specific ACC guidance is followed (and constitutes presumptive RCSC compliance), companies should document the use of RCSC guidance documents in their Code implementation efforts. Although the company’s own documentation need not be painstakingly detailed, it should indicate clearly (to the extent feasible) that the security actions employed throughout the company to address a potential terrorist attack were selected and implemented in conformity with, and in furtherance of, Code implementation.

2. Companies should utilize the various RCSC oversight mechanisms identified in the Designation, such as implementation progress reports, audits and third-party
verifications— and any documents that flow therefrom—to reemphasize the companies’ compliance with the Code. First, of course, such oversight measures should be identified as being performed for the purpose of implementing the Code as a QATT, as set forth in the Designation. Second, such oversight mechanisms provide valuable opportunities to reaffirm the nexus between specific actions and the Code—especially, for example, insofar as an “independent, accredited third party” creates an audit report recognizing or verifying how specific company or facility security measures serve to implement the Code. Specificity in these audits and verifications about how the security activities successfully implement the Code requirements could be quite helpful assuring that the Designation applies to these activities.

3. Finally, companies should clarify the ways in which compliance with the Code goes hand-in-hand with other related regulatory schemes, such as the Maritime Transportation Security Act (“MTSA”) regulations, 33 C.F.R. Pt. 305; Chemical Facility Anti-Terrorism Standards (“CFATS”), 6 C.F.R. Pt. 27; and security regulations for transporting hazardous materials by rail, 49 C.F.R. Pts. 172, 174. Given the overlap, companies should document how the specific actions taken to comply with these other regulations are not only consistent with but integral to the companies’ compliance with the Code.

V. What should an ACC member company do if they want more information?

ACC recognizes that its member and Responsible Care® Partner companies may require additional guidance based on their unique Code implementation circumstances. ACC will develop a Frequently Asked Questions (FAQ) document to address any particular circumstances in greater detail based on the member and Responsible Care Partner company inquiries it receives.
VI. Frequently Asked Questions

Question: Our Company implements the Security Code in all our divisions, including those that are not part of the ACC dues base. Does the Safety Act designation cover these parts of our company?

Answer: If a company has a division that is not part of the dues base, that division does not subject itself to the second component, “the oversight of the implementation of the management system”. Company divisions that are part of the ACC dues base implement the second component through the use of independent third party audits, the ACC governance process and potential expulsion from ACC or removal of partner status. Accordingly, divisions that are not part of the ACC dues base would not be covered by the SAFETY Act designation.

Question: We have sites outside the US that implement the Security Code and have been certified to RCMS®. Are these covered in the designation?

Answer: If a company has a site that is not part of the dues base, that site does not subject itself to the second component, “the oversight of the implementation of the management system”. Company sites that are part of the ACC dues base implement the second component through the use of independent third party audits, the ACC governance process and potential expulsion from ACC or removal of partner status. Accordingly, sites that are not part of the ACC dues base would not be covered by the SAFETY Act designation.

Question: If a terrorist attack was to occur at a facility that had implemented the Security Code, but was not part of the company’s sample of certified sites, would that facility be covered by the SAFETY Act?

Answer: Assuming that a company can affirmatively demonstrate that the three components of the technology were fully implemented or utilized at the facility at the time the terrorist attack occurred, and notwithstanding complete compliance with the Security Code, the attack still occurred, the legal protection afforded by the designation is available. It is for this reason that a facility’s documentation of all Security Code implementation and compliance activities is of utmost importance.

Question: Our Company joined ACC last month, we are dutifully implementing the Security Code at all our facilities and implementing RCMS®, if a terrorist attack occurred before we have completed our implementation plan, are we covered by the Security Act designation?

Answer: Generally speaking, implementation of the Security Code is a gradual process. If a terrorist attack occurred before there was complete implementation of the Security Code, the legal protection that the designation affords would not be available, as the designation
requires the complete implementation of the security management system. Although, under the terms of ACC membership, a company has three years to fully implement Responsible Care® at its facilities, the ability to obtain SAFETY Act liability protection is an incentive to complete the process sooner.

**Question:** Is a company required to show evidence that it has made use of every guidance document listed in the Safety Act designation (Appendix A) or do we have the ability to pick and choose which ones are best for our organization?

**Answer:** Under the Security Code, a company has the ability to select security measures appropriate for the needs of each facility. ACC provides a number of guidance documents to assist in this activity and these documents are listed in the SAFETY Act designation. In addition, the Security Code does not mandate compliance with all the guidance documents. As long as the company is using the documents listed in the designation to guide implementation of the Security Code, the company has satisfied the requirement, as per the designation, to implement a security management system, and the liability protection afforded by the SAFETY Act would be available.

**Question:** Is the Safety Act designation something our company should publicize to our stakeholders?

**Answer:** The Department of Homeland Security has stated that the purpose of the SAFETY Act and its protections is to facilitate and promote the development and deployment of anti-terrorism technologies that will save lives. By implementing and maintaining compliance with the Security Code, a company is demonstrating its ongoing commitment to deploying an effective anti-terrorism technology – one that has been recognized by DHS and afforded special liability protections because of its value and efficacy. While each company has its own corporate message that it conveys to stakeholders, the message of commitment to enhancing homeland security is one that is positive and that DHS clearly supports.

**Question:** Does the SAFETY Act cover chemicals being delivered to a customer?

**Answer:** The designation states that the Technology “enhances the ability of an ACC member or Partner to deter, detect, delay... to a physical or cyber attack against any form of chemical operation, whether at a fixed facility or during transportation. . .” . If a member’s or Partner’s obligation under the Security Code would include the protection and security of deliveries, such that deficiencies in the security of deliveries would be addressed under the ACC governance system, then the liability of the member or partner stemming from an event that occurred in the course of a delivery could be protected. However, if a company did not extend Security Code activity throughout the value chain, then delivery activity would not be covered under the SAFETY Act.
**Question:** As a railroad Responsible Care® Partner, would ACC assume our liability in the event of a security breach which resulted in a release of hazardous materials?

**Answer:** The SAFETY Act designation explicitly covers Responsible Care Partners. Accordingly, assuming that a Partner can affirmatively demonstrate that the three components of the technology were fully implemented or utilized by the Partner at the time the terrorist attack occurred, and notwithstanding complete compliance with the Security Code, the attack still occurred, the legal protection afforded by the SAFETY Act is available.

**Question:** I looked in the SAFETY Act and did not see any discussion of liability protection for downstream users of the technology. What is the source for that?

**Answer:** The SAFETY Act states “There shall exist a Federal cause of action for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the seller.” The Department of Homeland Security, in its preamble to the implementing regulations for the SAFETY Act, stated that this language means: a) only one cause of action exists for non-performance of the technology in relation to an act of terrorism; and, b) the cause of action can only be brought against the seller of the technology, and NOT buyers or downstream users of the technology. DHS states that Congress’ intent was to balance the need to provide recovery to plaintiffs against the need to ensure adequate deployment of anti-terrorism technology. This was done by creating a cause of action that provides a certain level of recovery against the seller, while at the same time protecting others in the supply chain.