The Heritage Foundation

ISSUE BRIEF

No. 4662 | MARCH 9, 2017

Expand the SAFETY Act to Make the U.S. More Secure

Brian Finch and David Inserra

The Support Anti-terrorism by Fostering Effective Technologies Act or SAFETY Act has been one of the Department of Homeland Security's (DHS) success stories. The SAFETY Act and its promise of liability protection following the devastating events of a terrorist or cyber attack has been warmly embraced by the security community as a whole.

However, for all its success, the SAFETY Act could still be better implemented by DHS, particularly when it comes to cybersecurity tools. Congress should also look to expand the SAFETY Act, including seeking to pilot an expansion to a country like Israel.

SAFETY Basics

The SAFETY Act provides creators of security tools and services with liability protections from damages incurred during an "act of terrorism," thus encouraging the development and deployment of such products to enhance the security of the nation. Under the SAFETY Act, any product or service that can be used in part to deter, defend against, respond to, mitigate, or otherwise combat an act of terrorism is eligible to receive specific liability protections.

The liability protections come in two forms: "Designation" and "Certification."[1]

This paper, in its entirety, can be found at **http://report.heritage.org/ib4662**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

Designation provides:

- Exclusive federal jurisdiction over all claims arising out of or related to an "act of terrorism" that involve a SAFETY Act–approved product or service;
- A bar on punitive damages;
- A bar on prejudgment interest; and
- A cap on liability for claims arising out of or related to the act of terrorism equal to some portion of the SAFETY Act–approved seller's/deployer's insurance policy.

Certification provides:

- All the same liability protections as a designation; and
- A rebuttable presumption of immediate dismissal of terrorism-related claims.[2]

These protections are intentionally powerful, as Congress was more interested in the deployment of effective and useful security products and services—thus decreasing the likelihood of terrorist attacks—than in years of legal disputes over responsibility for the success of any such attacks.

SAFETY Act protections formally become available when the Secretary of Homeland Security declares that an "act of terrorism" has occurred. In this context, "act of terrorism" is very broadly defined, covering:

- "Unlawful events" that cause harm, including economic harm, to persons, property, or economic interests in the U.S.; and

- An attack in which weapons or other instrumentalities intended to cause harm are used.

Note that this definition does not require that the "act of terrorism" be carried out by a "terrorist" group, only an individual or group intending to cause harm.

What the Administration Can Do to Expand the SAFETY Act to Cybersecurity

The success of the SAFETY Act as a whole is evidenced by the variety and number of companies that have taken advantage of the program over the past 14 years.[3] SAFETY Act applications have been approved for chemical-detection agents, bomb-sniffing dogs, explosive-detection devices, and security-guard companies. Many security-service offerings, ranging from risk-assessment tools to security-engineering and design programs have also been awarded SAFETY Act protections. The SAFETY Act covers more than just government contractors—professional associations, sports leagues and teams, owners of iconic real estate, and chemical companies have all received SAFETY Act protections.

Thus far, however, cybersecurity product developers and service providers are woefully underrepresented in the nearly 900 successful SAFETY Act applications. Indeed, only a fraction of SAFETY Act awards thus far have been to technologies that defeat malware or programs designed to mitigate the impact of cyber attacks.

A number of reasons are behind the slow uptake of the SAFETY Act by the cybersecurity community, not the least of which has been the relatively recent awakening to the scale and scope of cyber threats. Whatever the reason, the new DHS administration under Secretary John Kelly should move to supercharge the use of the SAFETY Act.

DHS can begin this process by noting that it has already awarded SAFETY Act protections to a small but vibrant set of cybersecurity technologies (e.g., advanced malware-detection programs). In addition to simply talking about the program, DHS can make it an integral part of its public-private partnership programs. This would include:

- Use of the SAFETY Act in the context of information sharing;

- Adoption of cybersecurity programs that exceed regulatory requirements; and

- Growth in confidence for customers and users who receive a SAFETY Act award.

Another major factor in the slow uptake of the SAFETY Act is the lingering misperception by many that the SAFETY Act does not apply to cyber attacks or to cybersecurity tools and services. Nothing in the law or the final rule implementing the SAFETY Act could be construed to limit its application to "traditional" terrorist methodologies. In fact, the preamble to the SAFETY Act Final Rule specifically discusses how the law applies to cyber attacks.

Still, a decent portion of the cybersecurity community will undoubtedly be reluctant to believe that the law applies to cybersecurity. In order to remedy that perception, Secretary Kelly should clearly state that the law as written can apply to cyber attacks, regardless of whether they are conducted by a group like ISIS or al-Qaeda.

What Congress Can Do to Expand the SAFETY Act to Cybersecurity

Even with the explicit pronouncements by the Secretary and his staff, doubters may still point

1. Homeland Security Act of 2002, Public Law 107–296.
2. Plaintiffs can only defeat that presumption of dismissal by (a) showing fraud or willful misconduct in the submission of a SAFETY Act application to DHS or (b) demonstrating that the claims do not relate to the SAFETY Act–approved product or service. A unique feature of the SAFETY Act is that plaintiffs may sue only the company that sells or deploys the product or service for alleged failures of those items. In other words, companies that buy or use SAFETY Act–protected tools/services may not be sued for buying "the wrong thing" or hiring "the wrong company." The reason for that additional layer of protection is to encourage companies in need of security services and tools to buy items that have been vetted by DHS through the SAFETY Act process.
3. U.S. Department of Homeland Security, "SAFETY Act: Approved Technologies," February 1, 2017, https://www.safetyact.gov/jsp/award/samsApprovedAwards.do?action=SearchApprovedAwardsPublic (accessed February 10, 2017).

to the lack of the word "cyber" in the SAFETY Act statute as a reason to question its utility. Many may also express concerns that the Secretary will have to declare a cyber attack to be an "act of terrorism" in order to trigger its liability protections.

The simplest way to resolve this situation is for Congress to clarify and update the SAFETY Act. A relatively simple adjustment to the statute can end lingering concerns about the narrow applicability of the SAFETY Act. Instead of only being allowed to trigger the SAFETY Act by declaring an event an "act of terrorism," Congress should give the DHS Secretary the option to declare an event a "cyber incident." The underlying factors (e.g., unlawfulness, actual harm, and intent to cause harm, etc.) would remain the same, only the words of the declaration would vary. This change would not be an expansion of the law; rather, it would just add a different term for describing an event that already triggers SAFETY Act protections.

Congress should also seek to expand the SAFETY Act beyond the U.S. as it is not the only country producing advanced and novel security services and technologies. By working with other countries, the U.S. can benefit from more products and also increase the market for U.S. products.

A good pilot country for this expansion of the SAFETY Act would be Israel, which has a vibrant security industry, a legal system similar to that of the U.S., and a small economy. After seeing how the pilot program works and working out the details, the U.S. could then consider expanding the program to other allies, such as Canada and Great Britain.

Advancing SAFETY

To improve U.S. security and cybersecurity, the President and Congress should:

- **Use existing authority to clarify that cybersecurity products can receive SAFETY Act protection.** While the terminology is not always clear, DHS should use its authority to apply SAFETY Act protections to cybersecurity products that attempt to prevent or mitigate unlawful events carried out by means intended to cause harm.
- **Clarify the existing statute to allow the Secretary to declare a "cyber incident" in order to activate SAFETY Act protections.**
- **Pilot a reciprocal expansion of SAFETY Act protections with a willing ally such as Israel.** To this end, Congress should provide the President with the authority to enter into an agreement with an ally to provide reciprocal liability protections.

Security and SAFETY at Home and Online

The SAFETY Act is an important tool to ensure the U.S. has the security products it needs to better prepare for, prevent, and mitigate the effects of terrorist attacks against the U.S. But the act has also been sparingly used to encourage the development of cybersecurity products. The U.S. should make it clear that the SAFETY Act covers cybersecurity products as well as seeking to partner with allies and partners in expanding the program. Doing so will make the U.S. even better prepared to face the threats facing the nation.

*—**Brian Finch** is Partner at Pillsbury Winthrop Shaw Pittman LLP and Senior Fellow at George Washington Center for Cyber and Homeland Security. **David Inserra** is Policy Analyst for Homeland Security and Cyber Security in the Douglas and Sarah Allison Center for Foreign Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*