Last revised October 2, 2018

Cyber SAFETY Act Coalition

Cyber technology companies are protecting America. Are you protecting them?

Recommended Edits to Substitute Amendment to S. 2392, the Cyber SAFETY Act of 2018 (ALB1870, June 12, 2018)

1. Declared Cyber Incident (Requirements)

Original language

> "(iii) causes national level impact and extraordinary physical or financial damage, harm, or disruption to— . . . ." (pg. 5, lines 3–5)

Proposed edit(s)

> 1st choice: Delete the reference to "national level impact."
>
> "(iii) causes ~~national level impact and~~ extraordinary physical or financial damage, harm, or disruption to— . . . ." (pg. 5, lines 3–5)
>
> 2nd choice: Delete "national level" and insert "widespread."
>
> "(iii) causes widespread and extraordinary physical or financial damage, harm, or disruption to— . . . ." (pg. 5, lines 3–5)

The Cyber SAFETY Act Coalition (the coalition) believes that the geographic stipulation in the substitute amendment (i.e., "national level impact") to S. 2392 is unnecessary and contrary to the SAFETY Act (SA).

- On the one hand, the 2006 final rule that underpins the SA rejects the need for a geographic requirement in the definition of an act of terrorism. On the other hand, the coalition recognizes that bill writers want to elevate the bar for triggering a declared cyber incident to ensure that relatively common cyberattacks are not granted protections.

- However, the bar should not be set so high that SA protections are unachievable by stakeholders whose technologies have been rigorously vetted and approved by DHS. After all, the SA applies to all terrorist events, large or small, with no category specifically reserved for national-level crises. Granting parity between physical terrorism and cybersecurity incidents is necessary and appropriate.

- The Cyber Incident Severity Schema in the *National Cyber Incident Response Plan* (NCIRP) captures the range of incidents—particularly level 3 (high) to level 5 (emergency)—that could prompt SA protections for covered technologies. Events in these levels would likely, if not definitely, impact U.S. public health/safety, national security, or economic security in powerful ways. The schema could help set the threshold for a declared cyber incident.

SAFETY Act Final Rule (June 8, 2006)

G. Definition of "Act of Terrorism"

. . . . The definition of the term "Act of Terrorism" set forth in the SAFETY Act provides that any act meeting the requirements specified in the Act, as such requirements "are further defined and specified by the Secretary," may be deemed an "Act of Terrorism." In the interim rule, the Department presented its view that the term "Act of Terrorism" potentially encompasses acts that occur outside the territory of the United States.

The Department stated that the basis for that view is "there is **no geographic requirement** in the definition; rather, **an act that occurs anywhere** may be covered if it causes harm to a person, property, or an entity in the United States." The Department confirms its prior interpretation. The statutory requirements for what may be deemed an "Act of Terrorism" address the legality of the act in question, the harm such act caused, and whether instrumentalities, weapons or other methods designed or intended "to cause mass destruction, injury or other loss to citizens or institutions of the United States" were employed . . . .

The Department **does not interpret** the language of the Act **to impose a geographical restriction** for purposes of determining whether an act may be deemed an "Act of Terrorism." In other words, the Act is concerned more with **where effects of a terrorist act are felt** rather than where on a map a particular act may be shown to have occurred . . . .

The focus of the "Act of Terrorism" definition on where harm is realized is appropriate in light of the possibility that an Act of Terrorism may be the result of a **series of actions occurring in multiple locations** or that the locus of the terrorist act may not be readily discernible. This is especially the case with respect to acts of **cyber terrorism** [bold emphasis added].

(Go to the next page.)

The National Cyber Incident Response Plan **(NCIRP)**
Annex B: Cyber Incident Severity Schema (pg. 38)

	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

Observed Actions	Intended Consequence[1]
Effect	Cause physical consequence
	Damage computer and networking hardware
Presence	Corrupt or destroy data
	Deny availability to a key system or service
Engagement	Steal sensitive information
	Commit a financial crime
Preparation	Nuisance DoS or defacement

2. Declared Cyber Incident (Judicial Reviewability)

"(A) IN GENERAL.—The term 'declared cyber incident' means any occurrence that the Secretary~~, in the sole and unreviewable discretion of the Secretary,~~ determines meets the requirements in subparagraph (B), as such requirements are further defined and specified by the Secretary." (pg. 4, lines 12–18)

The coalition urges bill writers to remove the reviewability language from the legislation.

- Both the underlying SA statute (P.L. 107-296) and regulation are silent on the issue of judicial review. Keeping the reviewability language in the legislation would weaken the incentive for businesses to *voluntarily* seek the liability protections of the SA. In turn, the wider ecosystem of entities (e.g., buyers and downstream users) that benefit from the safeguards afforded to sellers of qualified cybersecurity technologies would remain exposed to potentially crippling litigation.

- Over the course of several administrations, DHS secretaries have consistently declined to declare clear terrorist acts (e.g., the Boston Marathon bombing and the San Bernardino shooting) as acts of terrorism—effectively quashing the applicability of the SA to approved technologies.

- Some means of redress is needed. Indeed, the high standard for incidents to trigger SA declarations means that losses from such incidents would be of sufficient gravity to merit judicial consideration. Keeping the bill language silent on reviewability—maintaining the status quo—wouldn't give an advantage to either side of this issue.

- The coalition is open to considering committee report and/or statutory language clarifying that a declaration of a cyber incident is only for purposes of the SA and would have no impact on other U.S. government equities related to cybersecurity (e.g., the Terrorism Risk Insurance Act, or TRIA).

3. Declared Cyber Incident (Transparency, Application Process)

- The coalition believes that a clear process is required to facilitate DHS decision making concerning SA coverage determinations. Today, the department's approach for invoking the SA is opaque.

- It would be particularly problematic for DHS to deny SA protections by simply not addressing whether a significant cyber incident (e.g., a ransomware attack on a major U.S. city) rises to the level of a SA-declared cyber incident. Such *inaction* by the department would be profoundly detrimental to organizations that invest considerable resources in cybersecurity and SA safe harbors.

- To help the SA program fulfill its potential, DHS should write guidance and/or promulgate a rule on how an organization can submit a cyber incident for SA coverage. More transparency and interaction between SA-covered parties and DHS would improve the SA.