June 4, 2019

Via https://www.regulations.gov/docket?D=DHS-2019-0010

Mary Cantey
Department of Homeland Security
Science and Technology Directorate, Chief Information Office
245 Murray Drive, Mail Stop 0202
Washington, D.C. 20528

Subject: Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) comment request (docket number DHS–2019–0010)[1]

Dear Ms. Cantey:

The Cyber SAFETY Act Coalition, whose members represent nearly every sector of the U.S. economy, strongly supports the SAFETY Act program. We appreciate the substantial efforts that Department of Homeland Security's (DHS') Science and Technology Directorate (S&T) officials devote to managing the program, including vetting and approving SAFETY Act applications and meeting with the business community in multiple forums.

The coalition is pushing Congress to pass the Cyber SAFETY Act (CSA), along with increased funding for the SAFETY Act Office at S&T. This paper describes the need for CSA and presents a workable solution.[2]

Indeed, innovative cyber technologies are protecting America from foreign threats. The public and private sectors have a shared interest in ensuring that the SAFETY Act protects these technologies. CSA will facilitate the voluntary creation and deployment of leading cyber technologies that many stakeholders are demanding. Some cyber technologies may not be deployed except for SAFETY Act safeguards.

SUMMARY

- The Cyber SAFETY Act Coalition urges Congress to pass the Cyber SAFETY Act (CSA), together with increased funding for the SAFETY Act Office at the Department of Homeland Security's (DHS') Science and Technology Directorate (S&T). Innovative cyber technology companies are protecting America. The public and private sectors have a shared interest in ensuring that the SAFETY Act protects them from major foreign cyberattacks.

- Government and business entities confront relentless, often state-sponsored, cyberattacks. Industry continues to provide cutting-edge security for the common good, but it lacks evident government protection. This security gap calls for clear legal defenses.

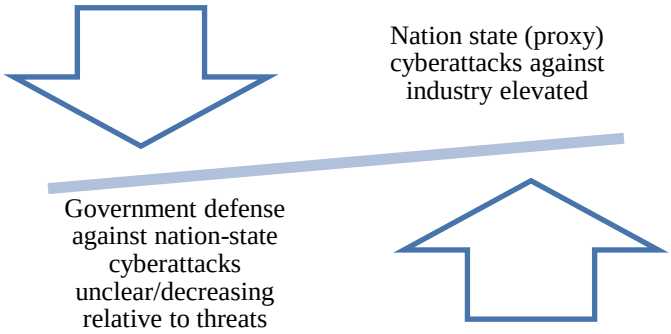
- CSA clarifies that the SAFETY Act applies to a significant cyberattack.[3] CSA does not simply absolve businesses of liability. Rather, it harnesses the SAFETY Act's carefully balanced approach to managing cyber risk and minimizing costly litigation.

- Some cyber technologies may not be deployed except for SAFETY Act safeguards. CSA technologies will reduce the magnitude of risk that the American public faces because of rampant cyberattacks.

- CSA will help incentivize companies to take their cybersecurity product, equipment, or service through DHS' rigorous SAFETY Act vetting process.

NEED: Public and private organizations are exposed to unrelenting, often state-sponsored cyberattacks, which are eclipsing the threat of physical terrorist acts.

- **The cyber threat landscape is causing government and industry to rethink homeland security.** On July 31, 2018, in announcing DHS' new National Risk Management Center, then-Secretary Kirstjen Nielsen described today's disturbing reality in cyberspace: "[C]yber threats collectively now exceed the danger of physical attacks against us. This is a major sea change . . . for our country's security."[4] The SAFETY Act was passed in 2002 to unlock the wider production and deployment of anti-terrorism technologies to protect U.S. businesses and institutions without fear of enterprise-threatening lawsuits, but only if the DHS secretary declared the attack an "act of terrorism."[5]



However, the legislation needs to be modernized to reflect that cyber assaults—whether undertaken by terrorists, state actors, or criminals—top the list of worldwide threats facing our nation.[6]

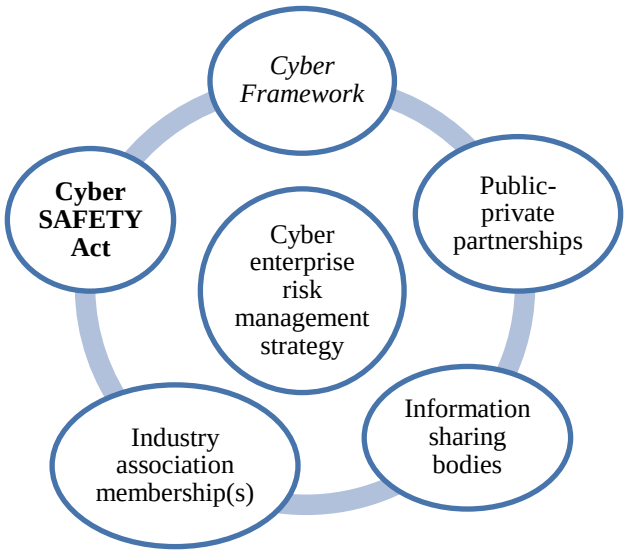
- **Businesses that provide security for the common good need clear government protection.** Despite the existence of dedicated homeland security, law enforcement, intelligence, and defense agencies, the U.S. government faces significant challenges in protecting industry from malicious hackers in the same way it does for physical threats.

  Cyberspace is the only domain where we ask private entities to defend themselves globally against foreign powers, other state-sponsored threats, and highly capable criminals.[7] While the military and police protect the land, sea, and air domains, in cyberspace, the private sector must do battle with national and criminal adversaries. Industry is frequently left holding the liability bag when malicious actors—including Russia, China, Iran, North Korea, and criminal gangs—successfully victimize businesses and related parties.[8]

  A high-level defense official told the U.S. Chamber of Commerce in May 2019 that industry is responsible for protecting itself from foreign cyber assaults, including ones from nation states, which justifies companies' need to pursue self-help solutions, particularly CSA.[9]

- **A security gap justifies making legal defenses plainly understood.** Since the U.S. government is limited in stopping destructive or disruptive attacks before they occur, CSA will help fill this chasm by clearly extending a safe harbor to state-of-the-art cyber technologies that are meticulously vetted and approved by DHS on an ongoing basis.

  CSA will be a key part of an organization's enterprise risk management strategy, which includes protections against acts of terrorism already available under the SAFETY Act; use of the National Institute of Standards and Technology (NIST) *Cybersecurity Framework*; participation in an information sharing and analysis center or organization; membership in a trade association that shares best practices; and partnerships with an array of government entities, such as the FBI or the Secret Service.



SOLUTION: CSA clarifies that the SAFETY Act applies to a significant cyberattack (i.e., a DHS-declared cyber incident) not already declared an act of terrorism. CSA will foster the voluntary development and deployment of cutting-edge cyber technologies that many stakeholders are calling for. Some cyber technologies may not be deployed except for SAFETY Act safeguards.

- **CSA modernizes—not expands—SAFETY Act liability protections to deal with high priority threats.** The SAFETY Act already includes information technology (IT) in the definition of a Qualified Anti-Terrorism Technology and offers liability protections for declared acts of terrorism—a point sometimes misunderstood by both advocates and critics of the SAFETY Act.

  CSA updates the SAFETY Act to more explicitly protect cybersecurity companies and related entities from potentially organization-threatening liability. CSA modernizes the protections already provided to voluntary sellers of approved cyber technologies that help shield the U.S. against cyberattacks launched by terrorists, nation states, and criminal organizations.

  To further support our nation's critical infrastructure entities—ranging from energy to financial services to manufacturing—the SAFETY Act should specifically say that a "declared cyber incident" will be covered by the statute's legal defenses.[10] Parties using cyber products or processes approved by DHS ought to be assured of SAFETY Act protections in the face of a demonstrable or significant cyberattack that could impact U.S. public health or safety, economic security, or national security.[11]

- **CSA coverage will generate beneficial externalities and a powerful win-win for the public and industry; CSA will create several positive externalities.** The rigorous, systemic SAFETY Act application process screens for cyber technologies that can detect, prevent, or mitigate cyberattacks with a comparatively high degree of certainty.[12]

  The extension of SAFETY Act protections will also increase the probability that CSA technologies are more widely deployed, reducing the magnitude of the public's exposure to a serious cyber event. The legislation will increase the research and development investments in these technologies, thus accelerating their appearance in the market.

  To obtain SAFETY Act protections, cyber technology sellers have to endure a lengthy and costly application process. CSA amplifies the SAFETY Act's message to those sellers: "Step up to raise the security and resilience of your product, service, or equipment—which DHS vets and approves—and the government will have your backs legally when you or your customers are attacked by malicious hackers."

  Such an outcome is a win-win for industry, policymakers, and the public. For years, public officials of both parties have strenuously appealed for improvements to cybersecurity technology, especially regarding Internet of Things (IoT) devices,[13] which CSA rewards.[14]

- **CSA safeguards do not simply absolve the private sector of liability.** Rather, CSA harnesses the SAFETY Act's existing, carefully calibrated approach to managing risk and litigation in an environment where cyberattacks are not declared an act of terrorism.

  - The SAFETY Act applies to a broad range of IT, including cyber products, services, software, and systems. CSA clarifies the SAFETY Act's liability limitations—including ones related to punitive and noneconomic damages, to claims arising from DHS-declared cyber incidents where SAFETY Act-covered cyber technologies are deployed, but an act of terrorism is not declared by DHS.

  - SAFETY Act-protected parties are the sellers of cybersecurity solutions; subcontractors, vendors, and suppliers that contribute to or market the SAFETY Act-approved cyber technologies; and users of such cyber technologies.

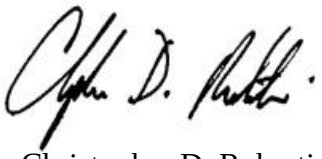
  - The SAFETY Act applies to a claim against the seller of a covered technology. Such a claim may only be maintained in a federal court. A similar claim may not be brought against the buyers, buyers' contractors, or downstream users of designated or certified cyber technologies (to the extent that the claim implicates the SAFETY Act-approved technology).

  - SAFETY Act protections don't apply if the seller's application is fraudulent or fails to have the requisite liability insurance to satisfy third-party claims.[15] Further, businesses could still be subject to contract-based claims, as well as administrative and regulatory claims.

***

The Cyber SAFETY Act Coalition welcomes the opportunity to provide feedback on the SAFETY Act. If you have any questions or need more information, please contact Christopher Roberti (croberti@uschamber.com, 202-463-3100) or Matthew Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,



Christopher D. Roberti
Chief of Staff
Senior Vice President, Cyber, Intelligence, and Security

Matthew J. Eggers
Vice President, Cybersecurity Policy

Cc: Senate Homeland Security and Governmental Affairs Committee
House Homeland Security Committee

Endnotes

[1] https://www.federalregister.gov/documents/2019/04/05/2019-06751/support-anti-terrorism-by-fostering-effective-technologies-act-safety-act#addresses

[2] The Cyber SAFETY Act (CSA) refers to S. 2392, the Cyber SAFETY Act of 2018, which the Cyber SAFETY Act Coalition wants to amend and pass. This legislation has not yet been reintroduced in the 116th Congress.
https://www.congress.gov/bill/115th-congress/senate-bill/2392

[3] Homeland Security Act of 2002 (P.L. 107-296), 116 Stat. 2242.
https://www.congress.gov/bill/107th-congress/house-bill/5005

Department of Homeland Security (DHS), "Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002" (the SAFETY Act final rule), *Federal Register* (June 8, 2006), pg. 33154.
http://www.federalregister.gov/documents/2006/06/08/06-5223/regulations-implementing-the-support-anti-terrorism-by-fostering-effective-technologies-act-of-2002

[4] DHS, then-Secretary Kirstjen M. Nielsen's "National Cybersecurity Summit Keynote Speech" (July 31, 2018).
https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech

[5] House Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies hearing *Promoting and Incentivizing Cybersecurity Best Practices* (July 28, 2015).
https://homeland.house.gov/hearing/subcommittee-hearing-promoting-and-incentivizing-cybersecurity-best-practices

House Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies hearing *Unlocking the SAFETY Act's Potential to Promote Technology and Combat Terrorism* (May 26, 2011).
https://homeland.house.gov/hearing/unlocking-safety-acts-potential-promote-technology-and-combat

Under the SAFETY Act, an "act of terrorism" is defined as such if it "(i) is unlawful; (ii) causes 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 (iii) 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." Homeland Security Act of 2002 (P.L. 107-296), 116 Stat. 2242.

[6] Department of Defense (DoD), "Cyber Tops List of Threats to U.S., Director of National Intelligence Says" (February 13, 2018).
https://www.defense.gov/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says

Aaron Boyd, "DNI Clapper: Cyber bigger threat than terrorism," *Federal Times* (February 4, 2016). https://www.federaltimes.com/management/2016/02/04/dni-clapper-cyber-bigger-threat-than-terrorism

[7] On September 27, 2017, former Secretary of Commerce Penny Pritzker said at the U.S. Chamber of Commerce that cyberspace is the "only domain where we ask private companies to defend themselves" against foreign powers and other significant threats. She wondered aloud, "Does that sound as crazy to you as it does to me?" https://www.commerce.gov/news/secretary-speeches/2016/09/us-secretary-commerce-penny-pritzker-delivers-keynote-address-us

The White House, *CEA [Council of Economic Advisers] Report: The Cost of Malicious Cyber Activity to the U.S. Economy* (February 16, 2018). https://www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy

Tony Bradley, "Gartner Predicts Information Security Spending To Reach $93 Billion In 2018," *Forbes* (August 17, 2017). https://www.forbes.com/sites/tonybradley/2017/08/17/gartner-predicts-information-security-spending-to-reach-93-billion-in-2018/#6ae4b1f63e7f

On August 13, 2018, MITRE released its *Deliver Uncompromised* report, which advances a "strategy for [DoD] supply chain security and resilience in response to the changing character of war." Among other things, the report calls on Congress to reduce businesses' litigation exposure by making it clear in legislation that the SAFETY Act applies to "cyber and supply chain security investments" (pgs. 39–40). https://www.mitre.org/news/press-releases/mitre-releases-deliver-uncompromised-study-on-confronting-new-asymmetric-threats

[8] DoD, *Final Report of the Defense Science Board Task Force on Cyber Deterrence* (February 1, 2017). http://www.dtic.mil/docs/citations/AD1028516

Charlie Mitchell, "Congressional oversight on cyber appears on pause until after election," *Inside Cybersecurity* (August 28, 2018). https://insidecybersecurity.com/daily-news/congressional-oversight-cyber-appears-pause-until-after-election

[9] The official's remarks were made under the Chatham House Rule.

[10] July 28, 2015, letter from the American Gas Association (AGA), the Edison Electric Institute (EEI), and the National Rural Electric Cooperative Association (NRECA) to the House Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies in support of "clarify[ing] the SAFETY Act to ensure that significant cybersecurity incidents are clearly covered under the program's liability protections."

[11] DHS' December 2016 Cyber Incident Severity Schema in the *National Cyber Incident Response Plan* (NCIRP) captures the range of incidents—especially level 3 (high) to level 5 (emergency)—that could prompt CSA protections for covered technologies. The schema could help set an appropriate threshold for a declared cyber incident. See NCIRP Annex B: Cyber Incident Severity Schema, pg. 38. http://www.us-cert.gov/ncirp

[12] See DHS working draft, *Use Cases in SAFETY Act Applications for Cybersecurity Technologies* (September 14, 2016).

[13] See Chamber testimony before the April 30, 2019, Senate Commerce, Science, and Transportation Committee Security Subcommittee hearing *Strengthening the Cybersecurity of the Internet of Things.* https://www.commerce.senate.gov/public/index.cfm/2019/4/strengthening-the-cybersecurity-of-the-internet-of-things

[14] For example, see Commission on Enhancing National Cybersecurity, Report on Securing the Digital Economy (December 1, 2016); S. 1691, the Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (introduced August 1, 2017); House Committee on Oversight and Government Reform Subcommittee on Information Technology hearing, "Cybersecurity of the Internet of Things" (October 3, 2017); Department of Commerce and DHS, *Report to the President on Enhancing Resilience Against Botnets* (May 30, 2018); and NIST, "Considerations for Managing IoT Cybersecurity and Privacy Risks Workshop" (July 11, 2018).
https://www.nist.gov/cybercommission https://www.congress.gov/bill/115th-congress/senate-bill/1691
https://oversight.house.gov/hearing/cybersecurity-internet-things
https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets
https://www.nist.gov/news-events/events/2018/07/considerations-managing-iot-cybersecurity-and-privacy-risks-workshop

[15] The final rule to the SAFETY Act says that causes of action "may be brought only against the Seller of the Qualified Anti-Terrorism Technology and may not be brought against the buyers, the buyers' contractors, downstream users of the Qualified Anti-Terrorism Technology, the Seller's suppliers or contractors, or any other person or entity. ..." The SAFETY Act final rule, pg. 33150.
https://www.safetyact.gov