Cyber SAFETY Act Coalition

Congress needs to swiftly pass S. 2392, the Cyber SAFETY Act of 2018

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

SUMMARY

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

2) S. 2392, the Cyber SAFETY Act of 2018 (CSA), **clarifies that the SAFETY Act applies to a significant cyberattack** (i.e., a "declared cyber incident") regardless of illicit actors' motivations.

3) CSA will **help incentivize companies** to take their cybersecurity product, equipment, or service through the Department of Homeland Security's (DHS') rigorous SAFETY Act vetting process.

   SAFETY Act labeling—i.e., a designation or certification—will **foster the voluntary development, purchase, and deployment** of cutting-edge cybersecurity technologies in threatening online environments, which many in the public are demanding.[1]

4) CSA does not absolve businesses of liability. Rather, CSA creates a **carefully balanced approach to managing cyber risk** and minimizing costly litigation.

   CSA will increase the likelihood that leading cyber technologies will be utilized because SAFETY Act protections are extended to the sellers and buyers of CSA technologies.

5) CSA will **create a positive security loop** involving cyber technologies being regularly tested and improved, businesses buying and deploying state-of-the art cyber technologies, and sellers and consumers benefiting from SAFETY Act protections.

   These actions should collectively prevent or limit the damage from significant cyberattacks against U.S. interests.

   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.

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 the Department of Homeland Security's (DHS') new National Risk Management Center, Secretary Kirstjen Nielsen described today's disturbing reality in cyberspace: "[C]yber threats collectively now *exceed the danger of physical attacks* against us [emphasis added]. This is a major sea change . . . for our country's security."[2]

  The SAFETY Act was passed in 2002 to unlock the wider production and deployment of anti-terrorism technology to protect U.S. businesses and institutions without fear of enterprise-threatening lawsuits, but only if the DHS secretary declared that terrorists committed the attack.[3]

  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.[4] CSA focuses on the impact of the cyber incident, not the identity of those who commit it.

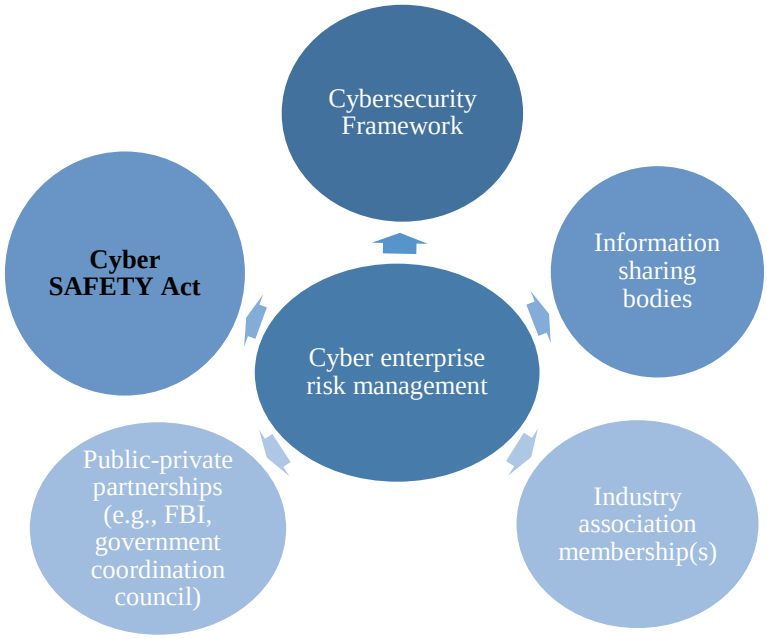
- **Businesses provide security for the common good but lack reliable government protection.** Despite the existence of dedicated homeland security, law enforcement, intelligence, and defense agencies, the U.S. government does not stand between industry and malicious hackers. Cyberspace is the only domain where we ask private entities to defend themselves globally against foreign powers, other state-sponsored threats, and highly capable criminals.[5]

  Leading enterprises are spending billions of dollars to provide security for the common good.[6] But there's a remarkable contrast between the proactive protection offered to the public by industry and the reactive efforts of government.[7]

- **Security gap justifies making legal defenses plainly understood.** Since the U.S. government doesn't stop potentially 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.

  The private sector has a legitimate frustration, which CSA will help lessen, that it is battling our nation's cyber adversaries almost single-handedly. Yet it is left holding the liability bag when malicious actors—including Russia, China, Iran, North Korea, and criminal gangs—successfully victimize businesses and related parties.[8]

  Worth highlighting, CSA will be a key part of an organization's enterprise risk management strategy, which includes 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.



The Cyber SAFETY Act will be a key element of a business' cyber enterprise risk management program.

SOLUTION: S. 2392, the Cyber SAFETY Act of 2018 (CSA), *clarifies* that the SAFETY Act applies to a significant cyberattack (i.e., a DHS-declared cyber incident). CSA will also 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 guards the voluntary sellers of approved cyber technologies that help shield the U.S. against cyberattacks launched by terrorists, nation-states, and criminal organizations.

  In addition, our nation's critical infrastructure entities—ranging from energy to financial services to manufacturing—need the SAFETY Act to specifically say that a DHS-declared cyber incident will be covered by the statute's legal defenses.[9] Parties using cyber products or processes approved by DHS ought to be protected in the face of a demonstrable or significant cyberattack that could impact U.S. public health or safety, economic security, or national security.[10]

- **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.[11]

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 SAFETY Act application process. Yet CSA essentially says to SAFETY Act beneficiaries, "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, which CSA rewards.[12] CSA answers this call.

- **CSA safeguards do not absolve the private sector of liability. Rather, CSA establishes a carefully calibrated approach to managing risk and litigation in an environment where the attribution of cyberattacks can be difficult to prove.**

    - CSA applies to a broad range of IT, including cyber products, services, software, and systems.

    - CSA extends liability limitations, including ones related to punitive and noneconomic damages, to claims arising from DHS-declared cyber incidents where CSA-covered cyber technologies are deployed.

    - CSA-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.

    - CSA applies to a claim against the seller of a covered technology. Such 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).

    - CSA protections won't apply if the seller's application is fraudulent or fails to have the requisite liability insurance to satisfy third-party claims.[13] Further, businesses could still be subject to contract-based claims, as well as administrative and regulatory claims.

Cyber SAFETY Act Coalition contact: Matthew J. Eggers, vice president, cybersecurity policy, U.S. Chamber of Commerce (meggers@uschamber.com)

Endnotes

[1] SAFETY Act marks range from Certification (red) to Designation (blue) to Developmental Test & Evaluation, or DT&E (green). https://www.safetyact.gov

[2] Department of Homeland Security (DHS), 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

[3] 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

[4] 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

[5] 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

[6] 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

[7] 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 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] See 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." https://homeland.house.gov/files/documents/AGA-EEI-NRECA%20support%20ltr%20B%20Finch%20SAFETY%20Act%20testimony%20HHSC%207-28-15%20FINAL.pdf

[10] 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

	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

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

[12] 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

[13] 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. ..." DHS, "Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002" (the SAFETY Act), *Federal Register* (June 8, 2006), pg. 33150.
http://www.federalregister.gov/documents/2006/06/08/06-5223/regulations-implementing-the-support-anti-terrorism-by-fostering-effective-technologies-act-of-2002
https://www.safetyact.gov

Homeland Security Act of 2002 (P.L. 107-296).
https://www.congress.gov/bill/107th-congress/house-bill/5005