LAWFARE
HARD NATIONAL SECURITY CHOICES

SECURITY BY DESIGN

Will a Cybersecurity Safe Harbor Raise All Boats?

Charlotte A. Tschider* March 2024

A private certification model, leveraging best-in-class cybersecurity assessment and audit practices, could be bolstered by public auditors and reinforced by downstream litigation models with relatively little cost to U.S. taxpayers.

INTRODUCTION

Supply chain cybersecurity incidents are incidents that compromise one party but affect another, and they now dominate the cybersecurity landscape. As organizations rely more often on third-party providers, the digital supply chain is one of the most significant risks to organizational security practices. Sixty percent of security professionals reported in a 2022 survey that third-party data breaches are increasing, and 59 percent of companies surveyed experienced a third-party data breach, the vast majority of which occurred in 2022.[1] Technology professionals cited lack of control, complexity, lack of resources to track third-party activities, third-party turnover, and lack of priority as key reasons for third-party, or "supply chain," risk.[2]

When supply chain cybersecurity incidents occur and consumers or business customers are harmed, litigation will likely result. However, the U.S. tort system, designed largely to address "wrongs" and allocate liability between parties, is rife with challenges that may punish responsible players and may enable organizations with poor practices to escape liability. In part, this is because the tort system is designed mostly for physical failures, not digital ones.

This paper argues for the use of a liability safe harbor consistent with industry standards and safeguards that will both improve domestic cybersecurity practices and reinforce confidence in business transactions. A private certification model, leveraging best-in-class cybersecurity

***Charlotte A. Tschider,** CISSP, CIPP/US, is an associate professor at the Loyola University Chicago School of Law.
[1] riskrecon, "Ponemon 2022 Study: Data Risk in the Third-Party Ecosystem" (2022), https://www.riskrecon.com/ponemon-report-data-risk-in-the-third-party-ecosystem-study, at 4.
[2] Id. at 7.

assessment and audit practices, could be bolstered by public auditors and reinforced by downstream litigation models with relatively little cost to U.S. taxpayers.[3]

In this paper, I first examine the unique nature of contemporary cybersecurity challenges, in particular the challenges of managing cybersecurity across a broad supply chain involving multiple technology players that may influence the security of a downstream product. Next, I briefly discuss liability challenges for the supply chain and describe why an alternative path may be needed. Finally, I examine how leveraging a private certification model as a liability safe harbor can provide consistent direction for courts resolving litigation between entities within the technology supply chain.

Specifically, I propose an executive order and associated statute that will establish a process for reviewing and approving preexisting, dominant, and extensive certification types already being used. It will also designate a safe harbor defense to liability for organizations that legitimately qualify for these certifications. Many of these certifications, funded by private organizations, have been used since the early 2000s as a basis for establishing trust between entities, such as those in a technology supply chain, and are well understood in the technology and service provider ecosystem.

A cybersecurity certification safe harbor can evolve and improve as adversaries and threat models inevitably change. If a safe harbor establishes a reasonable floor for expected cybersecurity practices but also provides reasonable updates over time, organizations using this safe harbor to avoid potential liability will collectively and consistently improve their cybersecurity practices. To accomplish this, as well as truly improve confidence in the digital supply chain, the U.S. must determine which certification models will adequately ensure these practices and certify associated certification-granting organizations.

Using cybersecurity certification as the basis for providing a complete defense to liability may not prevent every harm from occurring. However, if organizations invest in certification to avoid legal liability, this should collectively improve the resilience and quality of technology products in the United States and beyond.

CONTEMPORARY TECHNOLOGY RELATIONSHIPS ARE INFORMED BY PRIVATE OBLIGATION, NOT PUBLIC REGULATION

To understand why a certification safe harbor may be needed, it's important to understand how supply chain relationships are legally formed and where liability issues could arise. Historically, organizations creating digital technology products have enjoyed far less regulation than their physical counterparts. This is, in part, because digital technologies are not tangible products,

[3] A regulatory approach may indeed be a useful approach for artificial intelligence. See Eugenia Lostri, et al., "The Chaos at OpenAI Is a Death Knell for AI Self-Regulation," *Lawfare*, Nov. 28, 2023, https://www.lawfaremedia.org/article/the-chaos-at-openai-is-a-death-knell-for-ai-self-regulation.

which are subject to an established products liability legal model and recall mechanism.[4] With the exception of highly regulated industries like health care, finance, and government operations, only recently has the U.S. begun to seriously consider the potential for cybersecurity issues affecting a variety of data types and technologies across all industries.

Without robust regulation of digital products, organizations selling and purchasing technology have relied almost solely on private contracts to establish expectations of reliability, resilience, data protection, confidentiality, and desired function. The combination of digital technology products with physical embodiments (such as smart thermostats and children's toys) and the influence of digital technology products on impactful decisions (such as job applications, creditworthiness, and medical diagnostics) has revealed a common interest in safe, reliable technology products.

Despite a largely privately ordered technology ecosystem, the U.S. has identified the need for consistency and trust. To collectively improve the safety and reliability of technology products, organizational accountability is essential. As referenced in Pillar Three of the Biden administration's National Cybersecurity Strategy:

> We must hold the stewards of our data accountable for the protection of personal data; drive the development of more secure devices; and reshape laws that govern liability for data losses and harm caused by cybersecurity errors, software vulnerabilities, and other risks created by software and digital technologies.[5]

These needs are inevitable, but accountability is challenging because business organizations do not directly control the activities of other business organizations that produce portions of their systems and products. The sheer number of organizations involved in a single system's or product's supply chain makes accountability challenging. Open code, software, applications, apps infrastructure, and computing hardware are combined into broad systems and solutions. Modern computing solutions more closely reflect a manufacturing supply chain than their homegrown past. System architects and information technology development professionals are increasingly specialized in their expertise,[6] and computer systems regularly integrate and connect several different organizations' products into one system or solution.

Individual organizations that create technologies might know the most about their individual technologies, but they cannot always anticipate how these technologies will be integrated into downstream products or how they will be used in conjunction with other technologies. Even more, organizations that assemble multiple computerized technologies into a single system cannot know everything about each of the individual technologies in the final system, including

[4] Rachel Raphael, "Product Liability: The Upside of Recalls and Greater Industry Oversight," Crowell, Jan. 10, 2024, https://www.crowell.com/en/insights/publications/the-upside-of-recalls-and-greater-industry-oversight.
[5] The White House, *National Cybersecurity Strategy*, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, at 19.
[6] Chinmayi Sharma, "Setting a Higher Bar: Professionalizing AI Engineering," *Lawfare*, Dec. 12, 2023, https://www.lawfaremedia.org/article/setting-a-higher-bar-professionalizing-ai-engineering.

whether their combination has inadvertently introduced complementary vulnerabilities into the system, making it more likely to be compromised by cyberattack.

Each portion of these systems and solutions may be created by a different organization, subject to each organization's development practices and security programs. Reliability and security of the overall system or solution, then, necessarily depends on a number of other organizational decisions, which may be reasonable or unreasonable. Failures of portions of a system or solution that cause harm will likely be subject to litigation from a downstream organization or consumer, and at times it may be tremendously difficult to determine the origin of the problem.

One might expect that organizations could simply share information about their cybersecurity practices with other organizations in the supply chain. Presuming that organizations are even aware of the other entities that are part of a given supply chain for a system or product, organizations do not typically divulge information about their technology systems, either upstream or downstream.[7] The proprietary and confidential nature of this information, especially between competitors, remains a significant hurdle to collectively improving cybersecurity and technology development practices through information sharing. For these reasons, secure, resilient, and quality products require all members of the supply chain to individually employ reasonably comprehensive cybersecurity practices. However, there is currently no way of knowing whether these practices are consistent or not across the industry.

These challenges are not new; computer systems in recent times suffered from many of the same issues, but the complexity of the supply chain magnifies preexisting issues.[8] These issues do not just apply to downstream organizations building systems. Upstream organizations that license their technologies may have concerns similar to those of downstream organizations: They largely have no control or knowledge about how their technologies will be used downstream and whether they are adequately protected from upstream attacks. In a type of attack growing in popularity, cyberattackers may leverage poor downstream organizational or user security to compromise upstream products used by hundreds of customers, especially open-source code libraries, to maximize impact.[9]

Among calls for improved safety and security,[10] the U.S. should aim to satisfy two goals: (a) creating a system of accountability so that organizations and consumers have confidence in the

[7] Charlotte A. Tschider, "Locking Down 'Reasonable' Cybersecurity Duty," *Yale Journal of Law & Policy* 41 (2023): 77, 81–82, https://yalelawandpolicy.org/sites/default/files/YLPR/2._tschider_locking_down_reasonable_cybersecurity_duty.pdf.

[8] These issues are magnified in part by the dynamic inscrutability of artificial intelligence (AI), or its ability to self-learn with that self-learning being largely too complex for humans to understand. These issues are also magnified by the use of trade secrecy and confidentiality agreements, which make it comparatively more difficult for a technology user to evaluate AI before including AI in other systems or using it.

[9] Adam Bannister, "Upstream Attacks on Open Source Ecosystem up 400% as Criminals Seek to Compromise Applications at Scale," *The Daily Swig*, Aug. 12, 2020, https://portswigger.net/daily-swig/upstream-attacks-on-open-source-ecosystem-up-400-as-criminals-seek-to-compromise-applications-at-scale.

[10] Many of these concerns have been raised in relation to AI, as well, though these concerns are common to any technology system. White House, Executive Order 14110, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Oct. 30, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/. The National Institute of Standards and Technology (NIST) issued a request for comment on the executive order. The comment period was open until Feb. 2, 2024. NIST, "NIST's Responsibilities Under the October 30, 2023 Executive Order" (2023), https://www.nist.gov/artificial-intelligence/executive-order-safe-secure-and-trustworthy-artificial-intelligence.

safety and security of technologies they use or integrate in systems and solutions, and (b) streamlining the process for litigating inevitable downstream harms.

CURRENT LEGAL MODELS DO NOT EFFECTIVELY ESTABLISH NORMS FOR CYBERSECURITY BEHAVIOR

The primary legal mechanism for establishing any influence over other parts of the supply chain is through private agreement. Organizations purchasing or licensing code, infrastructure, applications, software, and the like establish their requirements through individual private agreements, but the degree to which cybersecurity requirements are included is often a matter of bargaining power and foresight. An organization with superior bargaining power could negotiate minor cybersecurity requirements for technology it provides to customers while requiring substantial cybersecurity requirements for its technology partners.[11] Some organizations, such as those with red teaming capabilities and cybersecurity bug bounties, might be better able to anticipate future cybersecurity issues, while others may be privy to such information.

Although the details of private agreements are typically subject to whichever organization has more bargaining power or information than the other, private agreements *can* influence security practices when they are used effectively. If a downstream licensee requires the license holder to contractually agree that it will conduct regular vulnerability scanning activities and distribute required patches on a timely basis, the licensing organization runs a substantial risk if it agrees to such a requirement without actually implementing it.[12] As part of these agreements, organizations include a requirement to certify to a specific certification standard and to maintain that certification throughout the life of the product, depending on the sector and type of product. However, in a supply chain that involves multiple organizations and products, it is not always clear which requirements have been established between two discrete parties.[13] In contrast, while certification requirements are familiar to most organizations involved in the digital supply chain, today, there are no formal requirements that apply to everyone across sectors.

When a cybersecurity incident or data breach occurs, it is somewhat inevitable that at least some organizations will attempt to resolve these issues in court and may use the agreement as the basis for breach of contract claims. They will also likely bring tort claims, especially if the plaintiff organization is not in privity with the defendant suffering a data breach.[14] However,

[11] I have experienced negotiating contracts with the same entity on both sides of the contract, with one organization requiring 50 pages of cybersecurity practices for my client. Two months later, my client negotiated with the organization for its services, where it refused any cybersecurity terms in the contract at all.

[12] Such an organization agreeing to a term it does not plan to implement or that it has not implemented can expose that organization to a breach of contract action, misrepresentation, or potentially a failure to bargain in good faith.

[13] Some organizations have attempted to control the private contractual arrangements of subcontractors and other entities on the supply chain that could affect their overall liability. I have dubbed this "sub-privity," as through a private agreement, one organization attempts to control the private contractual terms between two separate parties over which it has no direct control. See Charlotte A. Tschider, *International Cybersecurity and Privacy Law in Practice,* 2nd ed. (Wolter Kluwer, 2023). Sub-privity terms usually involve language such as "organization will ensure sub-contractors adhere to terms no less stringent than those established within this agreement."

[14] In most cases, tort actions will be barred by the economic loss doctrine when such losses are financial rather than physically damaging.

courts may find it hard to determine which cybersecurity practices are objectively reasonable or required under the agreement. Would-be defendants may also benefit from plaintiffs lacking information about their practices. For example, plaintiffs may be required to demonstrate a breach of cybersecurity duty but not have enough information about the defendant's cybersecurity practices to effectively argue a breach of duty, breach of contract, or reasonable alternative design. In other cases, courts could overlook objectively strong cybersecurity practices simply because a cybersecurity incident occurred (a cybersecurity incident would not have occurred unless the practices were unreasonable).

Breach of Contract

In breach of contract actions between organizations, the court will typically rely on the written terms of the agreement to determine whether the defendant has breached a specific material term. Although organizations evaluating a technology provider's product for use in their downstream products or for their internal use may conduct a review, that review may not fully review any serious issues in the provider's cybersecurity product. Depending on the bargaining power of the plaintiff, it may or may not have negotiated specific cybersecurity practices. Many organizations rely on a broad confidentiality provision or limited reference to "reasonable cybersecurity practices" rather than dictating specific practices.

Sophisticated organizations negotiating contracts may require specific contractual terms, in detail, including a requirement to acquire and maintain as current specific certifications throughout the life of the contract. However, not all organizations include these terms in agreements or have the bargaining power to do so. If the technology provider has superior bargaining power, a licensing agreement may include liability caps or limitations on liability, and other recovery restrictions may complicate the ways in which organizations can recover when they are harmed.[15] Collectively, the outcome of a breach of contract action may be highly variable depending on the negotiating power of the parties and cannot establish persuasive, collective direction in terms of what cybersecurity practices organizations should follow.

Negligence and Products Liability

When cyberattacks result in harms that are not purely financial, plaintiffs may claim negligence or pursue a products liability action.[16] As a legal matter, negligence is defined as "conduct which falls below the standard established by law for the protection of others against unreasonable risk of harm."[17] Negligence can apply to any type of scenario where one party is harmed and the other could potentially be at fault for its failure to exercise reasonable care. Negligence claims

[15] Stacy-Ann Elvy, "Hybrid Transactions and the Internet of Things: Goods, Services, or Software?" *Washington & Lee Law Review* 74 (2017): 77, 118, https://digitalcommons.nyls.edu/cgi/viewcontent.cgi?article=1939&context=fac_articles_chapters.
[16] Although not all states have established the economic loss doctrine, most have. In these states, the economic loss doctrine prevents parties from bringing torts claims for purely economic damages, prompting parties to only bring breach of contract claims. When cybersecurity practices are not established in the contract, this nearly forecloses any recovery for plaintiffs.
[17] Restatement (Second) of Torts, § 282.

require a plaintiff to establish that the defendant failed to exercise reasonable care in relation to the plaintiff and that this failure is the cause of the plaintiff's injury.

Plaintiffs may also bring one of multiple products liability claims: failure to warn (based on inadequate, incorrect, misleading, or misrepresentative labeling), design defect (defect in design process that inappropriately measures potential risk for design benefit), or manufacturing defect (unavoidable defect in the manufacturing phase of a product before it hits the market). Each of these requires a distinct approach: For example, a manufacturing defect enjoys strict liability, which does not require any demonstration of reasonable or unreasonable behavior, just that a defect caused the plaintiff's injury.

There are several challenges associated with negligence and products liability claims, both for plaintiffs and for defendants. For example, in negligence cases, the plaintiff must establish what the defendant's duty to the plaintiff was, based on foreseeable harm, and that the defendant breached that duty (failed to exercise reasonable care). This may be very difficult to demonstrate when the defendant didn't specifically know of the issue or the actions of a criminal's planned activities. Although foreseeability may be characterized more broadly, a particular kind of attack or technology failure may simply not be foreseeable. The challenges of ascertaining attribution and attack vector details will likely make a foreseeability showing difficult, especially for plaintiffs with comparatively less information than the defendant suffering a cyberattack.

For defendants, foreseeability could also cut against strong risk management practices. Knowing the potential issues for technology and making risk-based decisions about that technology is a hallmark of strong governance practices that measurably reduce potential risk. However, knowing potential issues exist can also demonstrate foreseeability as to their occurrence. This may incentivize defendants to make fewer documented decisions about risk or to knowingly avoid assessing certain technologies, which does not reduce risk but may reduce potential liability.

In products liability design defect claims, plaintiffs may have great difficulty demonstrating a reasonable alternative design that would have provided similar benefits with fewer corresponding risks, a requirement for demonstrating the defendant's design would potentially cause harm. In products liability failure to warn cases, defendants may have had great difficulty anticipating all potential issues and warning about these risks, such as in products that involve AI.

Moreover, the lack of division between design and manufacturing for the development of technology products, as is common in iterative development models, makes manufacturing defect claims difficult to prove. These claims are premised not on overt choices by an organization but by mistakes that happen between design and use by a customer. For technology products, customers cannot reasonably avoid risks, but organizations continue to make choices during design and while refining functionality, fusing design and manufacturing as

one rather than two distinct phases. This means manufacturing defects might also be similarly difficult to examine in court.

In the event an organization or consumer plaintiff effectively can bring a products liability action, there may be other challenges. As an initial matter, states may differ in whether products liability actions may be available to plaintiffs bringing cases involving digital technologies. In some state courts, digital technologies that aren't physical, like a web application, cannot be considered products, while in others, digital technologies may be considered products subject to products liability claims. Some digital technologies may be used in only digital form, while others could be integrated into physical devices, yet one may be subject only to negligence claims, while the other may be subject to products liability claims.

This inconsistency in claims will likely create differing expectations in terms of what organizations must do to avoid liability and what burdens rest on plaintiffs.[18] Moreover, a question of what actions are sufficiently reasonable can create inconsistent incentives for development. When an organization is not clear about potential risks and how to avoid them, it cannot reasonably determine which limited risks are worth accepting to achieve greater innovation and which risks could compromise a system.[19]

A CERTIFICATION LIABILITY MODEL COULD CREATE CONSISTENCY IN CYBERSECURITY EXPECTATIONS

The highly variable nature of private contracts, inconsistency in what "reasonable" cybersecurity could mean for courts, the challenge of broad confidentiality in computing practices, and the necessity of trust in the technology supply chain may require an alternative liability model that does not rely as heavily on courts to determine reasonable cybersecurity practices.

Although private agreements have established highly variable requirements within the supply chain, they have also facilitated trust and some consistency of expectations through terms that require third-party cybersecurity certification. Certifications are used routinely by sophisticated entities and those in a relationship with these entities either as an alternative to fully assessing the cybersecurity of another organization's system or product or as additional verification of an organization's cybersecurity practices. However, because certifications are often expensive and not typically required by law, some organizations do not acquire them unless required to form a business relationship.

[18] For more discussion of products liability law as a beneficial model over negligence law, see Chinmayi Sharma & Benjamin C. Zipursky, "Who's Afraid of Products Liability? Cybersecurity and the Defect Model, *Lawfare*, Oct. 19, 2023, https://www.lawfaremedia.org/article/who-s-afraid-of-products-liability-cybersecurity-and-the-defect-model.

[19] Certification approaches balance the award of a certification holistically. An organization need not perform perfectly for all controls but rather needs to demonstrate sufficient performance across controls. This model permits some flexibility in thoughtful decision-making, including waiting to remediate lower risk items while encouraging remediation of other risks. The risk-benefit trade-off is an important long-standing notion in innovation of all kinds. See *supra* note 10.

This movement toward certification seems inevitable given the rich diversity of the technology supply chain. The growing needs of complex technologies, including specialized technology like AI, require trust and expertise in the digital supply chain to realize their potential and to propel innovation. Computer systems are an amalgamation of various hardware, software, components, applications, source code, and databases, connected through various networking arrangements, but very few organizations develop all of these technologies. Resulting systems are a combination of not only this array of technologies but also the organizations that created them and *their* cybersecurity risks.

Further, with a shift toward technology specialization and professionalization, it is increasingly difficult for downstream technology developers and assemblers to even understand all details of a technology's individual parts. After all, every third party that might be part of the supply chain for a downstream product has its own third parties, which have their own third parties. The supply "chain," then, is actually more of a web of relationships, and these relationships are not usually visible or evaluable by others in the web that could be affected by cybersecurity decisions made by any of these third parties.

The inability to freely share information, which is expected in arms-length transactions involving highly proprietary data and especially when entities do not have direct relationships with each, creates the need for a trusted intermediary to establish trust (or at least provide a symbol of trust) between entities that otherwise do not trust each other or may not have any relationship at all.[20] Independent assessment and audits are one method for establishing trust. The right certification model—which integrates tests of both static and dynamic cybersecurity practices (such as process-based cybersecurity coupled with risk-based application of these practices)—should be performed by objective, qualified auditors. These auditors should be directly overseen by a government body, which establishes consistency in application. It also has the added benefit of streamlining potential litigation when a cyberattack or other technology failure occurs.

To better understand why certifications may be useful in a liability regime, it is important to understand why certifications are useful in private relationships today.

Preserving Reputation

Certification may be included in contractual terms; and for some highly regulated and high-visibility organizations, providing current certification is the price for doing business. Large organizations concerned about reputational damage may also use their significant bargaining power to require smaller entities to obtain certifications. Overall, certifications today are used as a risk-mitigating strategy. By relying on a trusted assessor to validate the practices of an

[20] It is common in security practices to leverage an outside entity to establish trust between two entities. For example, Certificate Authorities (CAs) are third parties used to establish trust in web page authentication practices between a web page operator and an organization or person connecting to the page by issuing digital certificates. See Michael Labos, "What Is a Certificate Authority (CA)?" SSL.com, Jan. 5, 2014, https://www.ssl.com/article/what-is-a-certificate-authority-ca/. Or third-party penetration testers may be used to identify and verify a product's resilience to a certain form of cyberattack. While a licensing or purchasing organization may not see the results, it can verify that such a test has been completed on a regular basis.

organization with which it would like to do business, an organization can save time validating the organization itself. The presence of a neutral entity also ensures confidentiality.

Certifications are created by certificate-granting organizations. The assessment is actually performed by advisory and consulting firms that are registered to assess to each certification standard. These firms often provide accounting or financial services, but their, licensed audit professionals are certified in audit techniques of all varieties. For example, the American Institute of CPAs (AICPA) established the Statement on Standards for Attestation Engagements (SSAE) for the purpose of evaluating key metrics of trust in various environments, from financial report reliability to other computing environments.[21]

The SSAE assessment framework is used across sectors and is broadly adaptable for various organizations in the supply chain. Although SSAE has three different models of attestation, the SSAE 18 SOC 2 Type II is the gold standard, which measures conformance to SSAE 18 SOC 2 Type I controls over and extended time period (both standard process and that process's implementation and exercise in an organization).[22] Organizations usually select the SSAE to attract business customers or because an organization believes an external audit can reveal (and lend credibility to) security issues, prompting internal investment to fix them.

Demonstrating Compliance

Certifications are frequently used for the purpose of validating compliance with regulatory requirements. The Health Information Trust Alliance (HITRUST), a U.S. organization that has developed a well-known risk and compliance framework for health care, created a certification process for purposes of establishing an actionable measurement of compliance with the Health Insurance Portability and Accountability Act's (HIPAA's) Security and Data Breach Notification Rules.[23] HIPAA-regulated covered entities may contractually engage with technology "business associates," third parties that receive protected health information. For these contractual relationships, HITRUST certification provides an easier way to determine which business associates can demonstrate compliance with these rules.

HITRUST certification has a substantial foothold in the health care industry, and it is used extensively by both covered entities and business associates regulated under HIPAA. An estimated 81 percent of U.S. hospitals and health systems, as well as 83 percent of health plans use HITRUST certification.[24] Most of these covered entities require HITRUST certification from

[21] Meredith F. Piotti, "SSAE 19: Updates, Compliance & Benefits," Wolf & Company, P.C. (2023), https://www.wolfandco.com/resources/insights/ssae-19-updates-compliance-benefits/.
[22] Id.; see generally, AICPA, "Statement on Standards for Attestation Engagements," April 2016, https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf (describing practices for SSAE 18); Deloitte, "Providing Assurance Through SOC Reports" (2022), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-rfa-providing-assurance-through-soc-reports.pdf, at 3–4.
[23] Health Information Trust Alliance, "HITRUST for HIPAA" (2022), https://hitrustalliance.net/hitrust-for-hipaa/.
[24] Health IT Security, "Understanding the Import of HITRUST Certification in Healthcare," March 8, 2023, https://www.healthitsecurity.com/news/understanding-the-import-of-hitrust-certification-to-healthcare.

their business associates and bind their business associates contractually.[25] Those business associates may have other business associates, so HITRUST enables each of the members of the digital supply chain to demonstrate a degree of reliability in meeting HIPAA requirements.[26]

Another example of compliance validation by certification is for government cloud providers. Government agencies are required to comply with the Federal Information Security Modernization Act (FISMA), which requires agencies to comply with the National Institute of Standards and Technology (NIST) Risk Management Framework, associated controls, and procedures.[27] Cloud providers that do work on behalf of these agencies typically agree to follow FISMA requirements as part of their government contracts. The Federal Risk and Authorization Management Program (FedRAMP), created in 2011, is a certification established by the U.S. government that enables providers to demonstrate their compliance with FISMA and, following, NIST.[28] FedRAMP certifies third-party assessment organizations (3PAOs), which are independent nongovernmental third parties that conduct assessments and issue various reports for agency review following assessments.[29]

Qualifying for a Business Arrangement

One certification applies to organizations to qualify for a payment processing business relationship and allocate fines when an organization has not complied. The Payment Card Industry (PCI) Security Standards Council, which includes the card brands Visa, Mastercard, American Express, Discover, and the Japan Credit Bureau, developed the PCI Data Security Standards (PCI-DSS) in 2004. The PCI Security Standards Council's original goal was to reduce growing costs associated with payment card processing when cards were compromised and used to perpetuate credit card fraud, which required coverage for the fraud and costs to reissue cards.[30] Under the PCI-DSS, organizations must demonstrate they are compliant with the standards. To do so, they must pay a qualified security assessor and successfully complete a PCI assessment, resulting in a report on compliance, or face substantial fines.[31]

If organizations do not pay their fines or are pervasively noncompliant with the PCI-DSS, card brands and financial institutions can prevent organizations from processing payment cards completely. States including Minnesota (2007), Nevada (2009), and Washington (2010) have

[25] Although HIPAA does not provide for a private right of action where HIPAA is the basis of negligence per se claims, it may still establish a standard of care in some states.
[26] Id. Although HITRUST is not *de facto* considered "compliant" with respect to the Department of Health and Human Services's enforcement of HIPAA, it is far more detailed and actionable than the law itself.
[27] NIST Spec. Pub. 800-53A.
[28] FedRAMP, "Partnering With FedRAMP" (2023), https://www.fedramp.gov/assessors/.
[29] FedRAMP Marketplace, "About FedRAMP Marketplace" (2023), https://marketplace.fedramp.gov/products (listing forty current assessors at the time of writing).
[30] PCI Security Standards Council, "About Us" (2023), https://www.pcisecuritystandards.org/about_us.
[31] PCI Security Standards Council, "Qualified Security Assessors" (2023), https://listings.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors; PCI Security Standards Council, "Report on Compliance" (2014), https://listings.pcisecuritystandards.org/documents/PCI_DSS_v3_ROC_Reporting_Template.pdf; Noah Stahl, "How Bad Can PCI Compliance Fines Get? This Bad," Network Assured, May 8, 2023, https://networkassured.com/compliance/pci-compliance-fines-penalties/ (describing fines for small businesses as much as $50,000/month from acquiring banks, or in the millions for large retailers, illustrating the payment card costs when large companies experience a data breach).

also premised liability on whether or not organizations have followed the PCI-DSS (although Nevada is the only state that explicitly names it).[32]

Supplementing Regulatory Review

Regulators have also used certifications as part of their importation and clearance processes. The U.S. Food and Drug Administration requires manufacturers of pharmaceuticals, medical devices, food, tobacco products, animal feed, and more to demonstrate compliance with good manufacturing practices (GMP) for safety purposes, especially when conducting these activities outside of the United States.[33] Certifying bodies demonstrate their reflection of ISO (International Standards Organization) standards when applying to be a certifying authority.[34] France's ASIP Santé has formalized this for cybersecurity applicable to health data, requiring HDH certification, which is based on ISO 27001.[35] Certifications can also streamline regulatory processes. If regulatory authorities have established clear criteria for certifications and audit certification issuers, they will likely spend less time evaluating these criteria in any clearance or other process. Even if a regulatory authority is actively assessing an organization, certifications can provide an additional fail-safe.

Bolstering Trust-Based Relationships

Certifications are useful in supply chain relationships because, whether solely or in combination with contractual terms, they illustrate the existence of an organization's commitment to certain minimum practices. In cybersecurity, this likely means that an organization has a reasonably robust cybersecurity program, at least for the technologies in-scope for that assessment. The goal of providing a certificate to a business customer, for example, is to facilitate trust. Of course, there is always the risk that certificates could be provided without adequate evidence or using limited criteria. Not all certifications are alike, and assessors who are not obligated to follow certain ethical obligations may be influenced by the organizations that pay them.

Certifications are used heavily in highly regulated sectors, but many prominent, well-respected certifications are used by organization, across sectors, that are engaged in technology activities. These certifications are used to facilitate contractual relationships and to establish confidence that an organization has a reasonably reliable and secure technology, system, and infrastructure. For example, a HIPAA-covered entity, such as a health care provider, is more likely to trust a technology service provider handling its protected health information if that provider

[32] Minn. Stat. 325E.64; NRS 603A.215; CW 19.255.020. Notably, in its liability provision 19.255.020(3)(a), Washington references that liability will stand even if the injury is not physical.
[33] See, e.g., 21 § U.S.C. 321, et seq. (describing pharmaceutical GMP requirements); U.S. Food and Drug Administration, "The Accredited Third-Party Certification Program: Questions and Answers: Guidance for Industry" (describing the process for establishing accreditation as a certification body that can provide certification to food safety GMP).
[34] U.S. Food and Drug Administration, "FSMA Final Rule on Accredited Third-Party Certification," July 13, 2023, https://www.fda.gov/food/food-safety-modernization-act-fsma/fsma-final-rule-accredited-third-party-certification.
[35] ASIP Santé, "HDH Accreditation Reference System," June 2018, https://esante.gouv.fr/sites/default/files/media_entity/documents/asip---referentiel-daccreditation-hds----v1.1---en.pdf, at 2.

can demonstrate it is HITRUST certified. Facilitating trust is essential to technology growth, especially as organizations rely on start-ups and other new players in the digital supply chain.

CAN CERTIFICATIONS COLLECTIVELY RAISE ALL BOATS THROUGH A LIABILITY SAFE HARBOR?

Certifications today are used in private transactions between organizations, primarily the subject of contract law, with some limited regulatory additions. However, certifications could be used more extensively to streamline common-law liability issues, reduce court time, and create a more predictable liability model for organizations. There are multiple reasons why a certificate-based safe harbor would likely be popular among at least a subset of organizations within technology supply chains.

First, as described in the previous section, organizations are currently using many of these certifications already, with most of them well known and well respected within the cybersecurity community. Second, well-respected certifications involve assessors or auditors who are required to follow a professional ethical code, including assessment objectivity. Finally, many certifications reflect standard cybersecurity practices established by NIST and ISO. Of course, each certification is different, but a small number of certifications illustrate strong cybersecurity practices both in process and in application, including SSAE 18 SOC 2 Type II, HITRUST, PCI-DSS, and FedRAMP. It would be relatively simple to begin with certifications known to be fairly comprehensive and review potential new certifications on an annual basis for possible qualification.

Over time, approving certifications in this way would likely lead to organizations in the supply chain protecting themselves, prompting organizations to contractually require U.S.-approved certifications from third parties rather than weaker certifications prone to gaming and cybersecurity greenwashing. To reduce these concerns for U.S.-approved certifications, certified auditors must be engaged to conduct assessments. Resulting reports should also be finalized in watermarked format, preventing manipulation, and copies submitted to the federal government overseeing the certification program.

While there are concerns generally about the validity of certifications in demonstrating program effectiveness, certifications assessed by qualified auditors and overseen by a central government body would lend confidence to certification.[36] Certifications with the right controls, evidence, and oversight could be used to demonstrate reasonable fulfillment of a duty of care or even reasonable product design. For example, a defendant could respond to a plaintiff's argument for breach of duty of care or alleging alternative (safer) design by submitting an assessment report to demonstrate proof of reasonable care or design. This practice would provide certainty for defendants and incentivize good *ex ante* behavior that collectively reduces

[36] This model is more objectively verifiable than self-certification practices currently in use, such as the EU-U.S. Data Privacy Framework's (DPF's) self-certification registration process, though this certification process could also be adopted to demonstrate reasonable security practices to support a DPF self-assessment. European Commission, "Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows," European Commission Press Release, July 10, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721; Paul M. Schwartz & Karl-Nikolaus Peifer, "Transatlantic Data Privacy," *Georgetown Law Journal* 106 (2017): 115, 158.

risk to downstream customers. Although this alone would not create a regulatory basis for enforceable complete defense to liability, courts could adopt this model without such a regulation if the certification used is approved and overseen by a governmental agency.

Creating a reliable certification system will collectively improve organizational cybersecurity and other technology practices, while making practices more consistent. Enabling the use of certifications to offer some protection from liability would likely encourage investment in cybersecurity practices not only to protect organizational assets but also to achieve some predictability in potential legal action.

The remainder of this section outlines features that should be present in a successful, complete certification system.

Certifications should reflect reliable measures of confidence.

Participation in a certification process at this time should be voluntary but could become compulsory as state or federal laws are developed or updated. The presence of an approved certification process could adapt to support future laws that supersede or otherwise integrate this certification process into their ambits. As described later in this paper, to incentivize more organizations to pursue certification, the U.S. federal government should offer "safe harbor" status for those that have been certified.

To effectively function as a safe harbor that could be referenced in federal or state statute or might be observed by courts, the right certification process must satisfy multiple goals simultaneously. It must include evaluation of objectively reasonable practices that actually reduce risk to downstream organizations and users, rather than general, nonspecific practices. Specifically, certifications that are properly scoped and involve both static and dynamic examinations of cybersecurity and technology development practices should adequately reflect *both* product-level confidence and confidence in broad organizational practices necessary for maintaining ongoing product confidence.[37]

Certification processes should provide confidence in technologies when an organization does not have the expertise to evaluate each technology individually or the time to spend evaluating upstream technology providers. This means certifications must be comprehensive and validated; in other words, any controls evaluated must have verifiable evidence that demonstrates compliance in action. Additionally, this evidence should be gathered or evaluated periodically to ensure such controls continue to be effective as technologies, vulnerabilities, risks, and threats undoubtedly change.

Although a bespoke U.S. cybersecurity assessment model might be desirable, existing certification bodies offer a more efficient way to accomplish the same goals while reducing

[37] See, generally, *supra* note 7 (describing the need for demonstrating both static duties, such as process-oriented cybersecurity practices, and dynamic duties, or processes as used in practice and as responsive to adversarial attacks, in determining what cybersecurity duties are objectively reasonable).

potential challenges and leveraging preexisting expertise. First, hiring the number of auditors necessary to staff independent certification within the U.S. government would be tremendously expensive and potentially impossible given a limited number of auditors in the U.S. (this model relies on private entities, which as explained is currently the case for many administrative bodies). Second, developing an independent certification standard would be time consuming and potentially not much more effective than existing models, many of which have already been evaluated by NIST.

Despite these challenges, establishing a model that *qualifies* existing certification bodies based on some standard expectations would minimize the need for administrative resources to conduct assessments. Moreover, because certifying bodies oversee their own qualification process for organizations to qualify as auditors or assessors, the qualification process could involve auditing these practices on a small number of certifying bodies rather than on every auditor or assessor.

Certifications should measure both process conformance and application within product scope.

A certification process should also evaluate the use of standardized practices as they are contextually used within given technologies, including processes that anticipate threats and vulnerabilities that will change over time. This means that, to successfully receive a certification, organizations will need to demonstrate specific application of processes not only over time but also in relation to specific threats and vulnerabilities. For example, a candidate for certification should directly demonstrate how it conducts vulnerability management, including by issuing vulnerability alerts and patching vulnerabilities, with respect to specific recently issued applicable vulnerabilities.

At a minimum, such certifications should require:

- Policies, processes, and procedures representing ISO and NIST cybersecurity domains (e.g., a vulnerability management policy and process) and annual training for all employees and contractors on the same
- Demonstrated evidence over a period of time of application of policies, processes, and procedures for all domains (e.g., vulnerabilities are evaluated, scored, and patches applied or remediation completed within a prescribed period of time based on score)
- Records of penetration tests completed for each in-scope system or product, conducted at least annually, and within thirty days following any material change
- A documented incident response process, incident response team, records of regular tabletop exercises, and recorded incidents with outcomes recorded
- A trained cybersecurity team with at least one dedicated employee responsible for cybersecurity activities

Multiple certifications could qualify if they meet these requirements.

The United States must audit the auditors.

Certification assessors must also be qualified and audited, and they must use only preapproved certifications. Effective assessment starts with a qualification process that ensures assessors perform a certification with qualified personnel and repeatable controls. Over time, organizations conducting assessments must also demonstrate a continuing ability to update their practices to newer versions of controls. Like the FedRAMP program, qualified, active assessors could be listed on a common federal website.

Of course, relying on certifications to demonstrate reasonable practices to the extent that they can effectively protect defendants against liability carries its own challenges. If certifications are reliable and evidence standardized, applied practices and assessors are qualified and audited, the main concerns regarding lawsuits are whether organizations maintained certification when the injury occurred. This concern is legitimate but is also verifiable. Certifications could be interrogated easily as part of negligence or products liability lawsuits.

There are existing government organizations that could theoretically audit certification bodies. The Offices of Inspector General—seventy-four individual bodies that are often created statutorily and currently charged with specific oversight—audit agency cybersecurity programs.[38] For example, the Department of Health and Human Services Office of Inspector General has a Cybersecurity and Information Technology Audit Division, which is the largest civilian audit agency, employing 600 professional auditors.[39] The Office of Inspector General could review which certifications an agency is recommending and ensure certifications are consistent with agency and statutory goals.

Alternatively, similar to FedRAMP, a Joint Authorization Board (JAB) could be formed, consisting of representatives from government agencies that determine which certification providers or certification types may be permitted.[40] FedRAMP also permits agencies to sponsor providers for faster approval.[41] This might mean that preferred certifications used to demonstrate cybersecurity compliance with certain laws, such as HITRUST for HIPAA, might be adopted quickly.

Implementing a complete defense to liability requires statutory implementation.

The challenge for implementing any defense to liability is that it generally requires a statute to provide this defense. A statute that provides for such a defense to liability could be passed for individual states or in federal law. One statutory model incorporating a defense to liability like this is the Cybersecurity Information Sharing Act of 2015, which authorizes companies to

[38] Kathryn A. Francis, "Statutory Inspectors General in the Federal Government: A Primer R45450," Congressional Research Service, Jan. 3, 2019, https://crsreports.congress.gov/product/pdf/R/R45450/4.
[39] U.S. Department of Health and Human Services, Office of Inspector General, Office of Audit Services Cybersecurity and Information Technology Audit Division, https://oig.hhs.gov/careers/office-audit-services-oas-cybersecurity-and-information-technology-audit-division-citad/.
[40] Tony Bai, "What Is FEDRAMP? Complete Guide to FedRAMP Authorization and Certification," Nov. 7, 2022, https://cloudsecurityalliance.org/blog/2022/11/07/what-is-fedramp-complete-guide-to-fedramp-authorization-and-certification/.
[41] Id.

implement cybersecurity controls that prevent cyberattacks and monitor the effectiveness of these controls.[42] The act also incentivizes sharing of incident data for purposes of improving national cybersecurity overall by protecting entities that disclose information from liability, both administrative enforcement actions and in federal court:

> No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 104(c) if—(1) such sharing or receipt is conducted in accordance with this title.[43]

The Cybersecurity Information Sharing Act premises any liability safe harbor on adherence to statutory requirements specified. For a statute creating a certification-based safe harbor, it would similarly need to be premised on certification requirements included in the statute and perhaps created by the statute. Although an executive order could potentially begin the process of establishing a national certification scheme, it would need to be statutorily reinforced to be binding on courts.

Although state excuses from liability could partially achieve a similar result, most cases involving a data breach of cyber incident will be heard in federal court due to their diversity status (plaintiffs and defendants residing in different jurisdictions) or their class-action status. Despite this, states could explicitly reference the federal certification scheme in statutes requiring "reasonable" security practices but lacking specificity in demonstrating compliance with such practices.[44] Even states that have established more granular security requirements, such as New York's Department of Financial Services Cybersecurity Law or the Stop Hacks and Improve Electronic Data Security (SHIELD) Act would not likely be inconsistent with certifications built on well-known standards.[45]

If an executive order creates a certification program, it could inform agency enforcement discretion and investigations. First, discretionary agency actions could be informed by certification to expressly demonstrate compliance where statutory compliance is subject to agency enforcement only, for example, the Federal Trade Commission (FTC), the Department of Health and Human Services Office for Civil Rights (OCR), or the Department of the Treasury's Office of the Comptroller of the Currency (OCC) enforcement actions under the FTC Act, HIPAA, and the Gramm-Leach-Bliley Act (GLBA), respectively.[46] While HIPAA and GLBA provide a

[42] Cybersecurity Information Sharing Act of 2014, S. 2588, 113th Cong.; National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066. 106(b).
[43] Id.
[44] See, e.g., California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.150(a)(1) (West, 2023).
[45] New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. Title 23, § 500 (2017); Stop Hacks and Improve Electronic Data Security (SHIELD) Act, S.B. S5575B, 2019-2020 Leg., Reg Sess. (N.Y. 2019) (enacted). The SHIELD Act offers specific controls that, de facto, put an organization employing these controls in compliance with SHIELD. It does not prescribe these controls directly or offer a private right of action.
[46] Of course, such demonstration of compliance would be evaluated by the agency, and such compliance schemes would need to adequately reflect required provisions of law. However, this approach could potentially create a more efficient investigation process for entities like the OCC, which is responsible for conducting bank audits on a regular basis, or for the OCR, which must conduct a heavy investigation when HIPAA complaints are filed or a data breach occurs.

statutory basis for evaluation (which certification could reflect), the FTC's broad enforcement authority could benefit from the structure a certification provides.[47]

Courts could also independently leverage qualifying U.S. certifications for purposes of demonstrating duty for negligence cases or satisfaction of reasonable alternative design for products liability cases. As I've described in a previous paper, a two-part evaluation of duty including both process satisfaction and reasonable exercise of that process should be invoked in data breach and cyber incident cases.[48] A certification scheme that includes both could similarly demonstrate reasonable behavior on behalf of a defendant (or lack thereof), while creating consistency between cases. However, courts would then need to establish some burden that shifts to defendants, as today plaintiffs are responsible for demonstrating breach of duty or existence of a reasonable alternative design that proximately (legally) caused their injury in fact.

Defense to liability must be limited initially to common-law torts.

As described above, certification will likely work most effectively for torts cases because these cases turn on a determination of objective reasonableness. Auditors reviewing the cybersecurity practices of an organization with respect to a system or product provide an objective measurement of such practices that are most likely to work effectively in these cases. However, it is possible that future regulation could also reference these certification practices as demonstration of compliance with a regulation, similar to the PCI-DSS referenced in state laws. Alternatively, certification could be included as a statutory requirement in limited cases where confidence in compliance is more challenging or the stakes are higher, such as with critical infrastructure or highly sensitive data.

Certification could be used to provide a complete defense to liability, but the legal mechanism and how it would functionally apply may differ depending on the type of tort claims a plaintiff brings. For negligence actions, defendants could provide evidence of current (at the time of the plaintiff's alleged injury), approved, scope-applicable certification in their answer to any complaint and in pretrial motions, such as a motion to dismiss. In the event a defendant cannot substantiate that it was in compliance with the certification requirements at the time of the compromise or technology failure, the plaintiff could be granted some latitude in its demonstration of the defendant's breach of the duty of reasonable care in pretrial motions. Then, the burden could shift to the defendant to demonstrate that its practices were reasonable, despite not being current with its certification at the time of the injury.

For products liability actions, a defendant's certification could provide evidence of reasonable design. For products liability design defect claims, a plaintiff is usually required to demonstrate that a reasonable alternative design existed. A reasonable alternative design is a design that

[47] See Justin (Gus) Hurwitz, "Data Security and the FTC's UnCommon Law," *Iowa Law Review* 101 (2016): 955, 972 (describing the flexible standards and norms under the FTC's unfairness prong that create a moving target for organizations subject to FTC investigation). Although a certification model, without more, does not achieve binding legal norms that conform to the Administrative Procedure Act, it could at least create greater standardization beyond case-by-case consent decree settlements. Court-based decisions will of course differ in their precedential function, but a similar standard could theoretically be used in both cases.

[48] See *supra* note 7.

would have worked as well as the design in question, which was possible technically at the time, with fewer risks of the type that caused the plaintiff's injury. If it is the plaintiff's burden to demonstrate a reasonable alternative design, then the defendant can respond by challenging the alternative design. The existence of certification can overcome liability when the defendant presents valid, scope-applicable certification. Similarly, a plaintiff could argue that the certification was not valid or did not apply to the scope presented.

It would be difficult to provide a complete defense for breach of contract actions as a court's evaluation is often based on interpretation of the terms of the agreement. However, with awareness to certification, courts may interpret an organization's use of U.S.-approved certification as performance of "reasonable" cybersecurity duties or reasonable practices to protect confidentiality when contractual cybersecurity terms are vague or nonexistent.

Of course, complete defenses to liability would be reflected primarily in federal courts, for example, in large class-action lawsuits. Although states may consider something similar, complete defenses to liability in class-action lawsuits in federal court could be extremely effective. Future class actions involving broad technology failures or cyberattacks will likely compromise multiple systems at one time or impact many consumers simultaneously.

Certification cannot be valid when compliance lapses or defendants attempt to expand its scope of application.

Reports of compliance or similar reports following a certification process's conclusion are used to demonstrate the effective certificate date and length of that certification, the entity that performed the certification, and the technology scope of the certification. Moreover, a material change in the technology usually requires timely recertification. These reports are important because they clearly demarcate the scope of the certification so that organizations cannot rely on the certification for products or systems that are not certified.

Additionally, these reports often include risks identified that are required to be remediated within a period of time and risks that have been accepted. For these reasons, reports must be provided to substantiate a complete defense to liability. In the event the case centers around technology, plaintiffs can probe the effective application of the certification and allege, for example, that the technology was not covered by the certification, that the technology has materially changed, that the incident causing the harm could have been prevented by remediating items listed in the report, or that the certification has lapsed.

Organizations do occasionally experience lapses in current certification status, and in some cases, organizations may not be fully certified for both their internal organizational practices and their products. In other cases, organizations may have an active certification, but they may not be adhering to the requirements of the certification when some harm occurs, for example, receiving vulnerability reports and timely patching systems.

Certification should be visible to promote adherence and facilitate trust.

Perhaps the most positive effect of certification-based defenses to liability is that certifications could be hosted on a public website for any organization holding its technology out for downstream use, which can also serve as a clearinghouse and starting point for potential technology relationships. This can be useful to organizational procurement professionals seeking low-risk third parties to perform any number of technology functions. With clear information available, potential business partners will be in a far better position to rely on these organizations without having to spend a great deal of time and money evaluating them. In the long term, certification could streamline the contracting process overall, while simultaneously simplifying litigation and enhancing actual technology practices.

Of course, with any solution come costs. Certifications are not cheap—they are more expensive with more comprehensive evaluation such as program review, testing of program application, and gathering of evidence. High-quality certifications usually require certified auditors, as well, which come at a high price. Moreover, organizations with large technology solutions will be more expensive. This is because upstream providers are developing technology that large technology solutions incorporate into their downstream products. However, downstream technology solutions could rely on upstream certifications to simplify their own downstream certification processes.

Downstream certifications today will often shortcut the review by integrating upstream providers' certifications into assessment scoring (if an organization works with certified upstream providers). This means downstream technology licensers of upstream technologies do not have to pay to certify certain portions of their product. It also protects the confidentiality of these technologies for upstream developers. Despite the costs for organizations, the significant number of audit and assurance organizations maintaining and auditing for these certifications could grow, improving membership, skill sets, and job opportunities in the United States.

CONCLUSION

The greatest benefit to a certification safe harbor is that it can, over time, create incentives to improve collective security practices. Many organizations prioritize investment in areas that can significantly avoid or transfer risk, especially legal risk. Organizations may feel uncomfortable taking on the risk of uncertified organizations (either cybersecurity risks or the potential of losing their certification), prompting vendors and other third parties to certify and maintain their organizational customers. An organization that decides to work with a noncertified upstream technology provider will have to do considerably more work in its own certification and internal assessment of the provider's practices to protect itself from liability.

Raising enough (cybersecurity) boats can measurably improve the quality, reliability, and security of a variety of different technology products and create trust between various entities that may wish to do business with one another. Over time, the selection of certified upstream technology providers over noncertified providers will likely influence the number of entities

getting certification. Because there is no such thing as a fully secure or perfectly performing system, injuries will still occur even if organizations complete certification. However, these injuries should occur less frequently and be less severe if organizations have implemented resilient, adaptable programs, and if certifying bodies evolve certifications as new threats emerge (as they have so far).

Although certification is not a perfect solution, it is an approach to risk management that is well known and currently used in the technology supply chain. Certifications increase trust between contracted organizations and downstream where organizations may not be able to evaluate all participants upstream. Certifications can also improve collective public interests, if they effectively measure both process-based security and information technology programs, as well as the application of those processes to the technology in question. The United States would do well to consider a certification-based liability safe harbor that incentivizes improved U.S. supply chain quality and cybersecurity that would improve consumer and organizational products.