Statement of Dr. Andrea M. Matwyshyn
Microsoft Visiting Professor, Center for Information Technology Policy, Princeton University/
Professor of Law, Northeastern University/
Affiliate Scholar, Center for Internet and Society, Stanford Law School
Before the
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Committee on Homeland Security
U.S. House of Representatives
July 28, 2015

Chairman Ratcliffe, Ranking Member Richmond, Representative Langevin, and other distinguished members of the Committee, it is my honor to be here with you today to discuss the future of information security in the United States and the SAFETY Act. My testimony today reflects cumulative knowledge I have acquired during my last sixteen years as both a corporate attorney and academic conducting research on the legal regulation of information security. My testimony also reflects the practical business knowledge I have obtained through long-standing relationships with insiders at Fortune 100 technology companies, technology entrepreneurs, consumer rights advocates, and independent information security professionals. Finally, this testimony is informed by insights acquired during my service as the Federal Trade Commission's Senior Policy Advisor/Academic in Residence, advising on matters of information security.

During the last decade, awareness of information security has dramatically increased in both the public and private sector, and state data security statutes have contributed significantly to this improvement. However, the field of information security is still in its early years, and the overall level of information security knowledge and care that currently exists in the United States is still inadequate. As high profile data breaches such as the security failures of organizations such as OPM and Sony permeate the news, citizen confidence in the data stewardship capabilities of both companies and government agencies is eroding. Dramatic information security improvements are necessary throughout both the public and private sector, and it is this social context that frames today's legal and policy conversation around the SAFETY Act.

The SAFETY Act's primary feature – a grant of limited liability to companies whose products are certified by the Department of Homeland Security and to their customers – is a poor fit for stimulating improvements and incentivizing adherence to best practices in information security. SAFETY Act certifications for information security products are not likely to lead to improved information security in either the public or private sector. Instead, such grants of limited liability for information security products and services are more likely to have the inverse effect. They are likely to unintentionally create incentives for lower quality in information security products and services, indirectly undermining national security and consumer protection advancement.

1. **Limitations of liability are likely to disrupt information security innovation in the marketplace – an outcome that contradicts the goals of the SAFETY Act -- and to create disincentives for corporate purchasing based on information security technical efficacy**

The marketplace for information security products and services has dramatically evolved since the passage of the SAFETY Act. While the SAFETY Act's liability limitation incentives for creation of new information security products may have been helpful in 2002, in 2015 they are unnecessary. The market for information security is robust and has matured significantly: according to some estimates, sales of digital security products and services are likely to approach $80 billion worldwide in 2015 and rise to $93 billion in the next two years.[1] Information security company companies are successfully obtaining venture capital easily and engaging in IPOs,[2] and high quality information security products are successfully appearing in the market. Because of this healthy market growth, any selective liability limitation incentives injected today by the SAFETY Act are likely to be undesirably disruptive and damagingly counterproductive to the successfully blooming market for information security products and services.

Because of the fast pace of innovation in information security, it is likely that the liability protection offered to certified products by the SAFETY Act will outlive the optimal technical efficacy of those certified products. Yet, any technology deployed during the period of designation is protected for the lifetime of designation. Indeed, the older a certified product becomes, the more outdated and potentially vulnerable it is likely to become, particularly because material changes may require DHS notification/refiling to maintain certification. Meanwhile, the SAFETY Act liability shield remains constant across time. Thus, it is precisely the older, potentially more vulnerable certified technologies that may command a lower price-point and superficially appear most cost-effective to corporate decisionmakers without technical expertise.

As a consequence, business purchasing incentives could undesirably shift away from maximizing best practices in information security in favor of maximizing liability limitation. Corporate CFOs and general counsels will be likely to override the technical judgement of the CISO and their information security engineers in at least a portion of corporate information security products purchasing decisions. Companies will therefore likely shift away from purchasing based primarily on technical efficacy toward purchasing information security products based on whether they are certified under the SAFETY Act, even when those certified products may be of inferior technical quality or a worse business fit. In granting limitations of liability to only certain information security companies under the SAFETY Act, DHS would unnecessarily manipulate an already-competitive information security marketplace, potentially hindering adoption of new information security technologies in favor of older ones.

A significant and growing portion of the information security expert community does not view the use of liability limitation approaches as the correct path to improving public and private sector information security. As vulnerabilities will increasingly lead to potential loss of human life,[3] code quality and information security rigor in products become paramount. Similarly, sophisticated technology companies with heavy investments in information security in many

[1] http://www.betaboston.com/news/2015/07/17/cybersecurity-firm-rapid7-raises-103m-in-years-first-boston-tech-ipo/
[2] Id.
[3] http://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

cases do not necessarily support limitations of security liability, and they are concerned that less ethical companies are misrepresenting the quality of the security in their products and services. Due to low enforcement and lack of information security liability, the market currently inadequately sanctions misrepresentations of information security quality in products and services. Liability limitation for information security products will only exacerbate this code quality problem, unfairly disadvantaging the companies who purchase the best-of-breed information security products based on technical information security concerns and enterprise fit rather than based on DHS certification.

Selective liability limitation through the SAFETY Act also disadvantages information security startups. Startups are most likely to be allocating resources to code development at the expense of allocating budget to the legal resources necessary to apply for a certification under the SAFETY Act. Yet, security startups sometimes offer the most appropriate product for a particular information security corporate need from a technical perspective.

2. The level of technical rigor in procedures in the SAFETY Act certification process are suboptimally transparent

Pursuant to my review of available information regarding the SAFETY Act certification process, the process of certification is currently suboptimally transparent. Available DHS materials raise material concerns regarding the technical rigor and thoroughness of the vetting process for certification of information security products and services. DHS states in informational materials on its website regarding the certification process that it views itself as "nonregulatory" and that a body of unidentified "technical experts" will provide "suggestions." The process appears to be largely applicant self-reported with respect to product and services performance and quality. It is not clear from available DHS materials that DHS performs any independent penetration testing, analysis of code quality, assessment of patching speed or quality review of self-reporting through prior applicant security advisories during the process of evaluating applications. Members of the information security research community have also raised various concerns regarding the process.[4] For example, my consultations with private sector vulnerability database experts have yielded potentially important unanswered questions regarding the quality of currently-certified information security products' advisory release history.[5]

An applicant-driven, non-transparent process is not optimal for a governmental process culminating in the substantial privilege of a grant of limited liability for harms resulting from information security inadequacy. When these process ambiguities are added to the suboptimally precise definitions in the SAFETY Act regarding the classification of security incidents and the broad discretion afforded to DHS in interpretation, substantial concerns exist regarding the current structure of the certification process.

[4] http://www.csoonline.com/article/2918614/disaster-recovery/fireeye-offers-new-details-on-customer-liability-shields-under-the-safety-act.html

[5] Interview with content managers at OSVDB.

3. **Grants of limited liability for information security products are likely to negatively impact timely patching, code integrity vigilance, and the quality of advisory disclosures in certified information security products**

DHS currently lacks adequate enforcement authority to require correction of corporate information security inadequacies or to stop companies from selling dangerously vulnerable products in the marketplace. In fact, as expressly stated with visible frustration in DHS advisories, companies feel at liberty to brazenly disregard DHS's demands for correction of even serious security vulnerabilities in their products and services.[6] Adding a layer of liability protection under the SAFETY Act for information security products would only exacerbate this bigger DHS enforcement problem, creating additional incentives for certified companies to neglect or delay patching or updating of their products.

Removing risk of liability eliminates an important corporate incentive for timely patching, internal vigilance regarding code quality and release of adequate security advisory notices. The primary information security challenge faced in the marketplace today is policing the consistent quality of information security products and services in light of their increasing vulnerability across time. Deteriorating quality and unpatched information security products create a false sense of security and leave their users vulnerable to attack. The liability limitations of the SAFETY Act do nothing to improve the quality and integrity of information security products. Instead, they potentially create perverse incentives for lower levels of product and services vigilance through a liability buffer for certified companies.

4. **Grants of limited liability under the SAFETY Act for information security products may indirectly disrupt information security enforcement work of other agencies, harming our economy and national security**

DHS's selective certification of particular information security technologies and grants of liability limitation may hinder the work of other agencies working to improve information security. In particular, the work of the Federal Trade Commission, Federal Communications Commission, Securities and Exchange Commission, and Consumer Financial Protection Bureau may be impacted. These and other agencies are currently expanding efforts to police the quality of information security and data stewardship offered by businesses to consumers and business partners. These agency efforts are still in their nascence in many cases, but ramping up swiftly. A limitation of liability would potentially meaningfully circumscribe these agencies' efficacy in using fines or disgorgements to obtain redress for consumer, businesses, and national security harms arising from information security inadequacy. This is an undesirable limitation on important work by other agencies aimed at improving information security in our economy.

[6] https://ics-cert.us-cert.gov/advisories/ICSA-14-084-01 ("Festo has decided not to resolve these vulnerabilities, placing critical infrastructure asset owners using this product at risk.")

5. **Limiting states' rights to impose liability for corporate information security misconduct will further erode consumer trust and damage innovation in the United States.**

Information is only as secure as the weakest link in the chain of possession. Therefore, it is essential that the highest possible floor of information security be created across organizations in both the public and private sector. However, the field of information security law is very young, and best practices of conduct continue to evolve rapidly. As such, determining the best legal regime for addressing information security liability will require experimentation on the state level to arrive at an optimal legal framework. A broader social and scholarly conversation on information security policy is desperately needed, and it requires time to develop. At this juncture I believe strongly that it is dramatically premature and undesirable to federally limit liability for information security misconduct demonstrating a lack of due care in any form, including through the SAFETY Act.

States have traditionally been the laboratories of experimentation for novel legal approaches to liability. The best course of action with respect to any consideration of limitation of liability is one exercising deference to federalism concerns and states' regulatory interests in redressing the harms of their citizens for information security harms. Different states engage with consumer protection questions in different ways, and no national consensus currently exists with respect to the best course of action for information security liability. Federally imposing the model of the SAFETY Act liability limitations undesirably breaks with the federalist tradition of deference to state liability determinations. It also disrupts the traditional deference of allowing state contract law to be the primary source of liability shifting determinations between contracting parties. Information security companies are usually represented by attorneys who may lack SAFETY Act expertise but who are amply capable of negotiating contractual limitations of liability with business partners, as are, in turn, the attorneys of the companies that rely on those information security. Contract and tort law are already beginning to adequately rise to the challenges presented by the information security marketplace, and federal intervention into software liability limitation is not necessary and premature at this juncture.

Thus, I strongly urge this Committee to exclude information security products and services from the SAFETY Act and avoid legal approaches driven by limitations of liability in information security. Selectively granted limitations of liability through the SAFETY Act will hinder innovation in information security and negatively disrupt the information security marketplace. They are also likely to indirectly damage national security and stifle consumer protection efforts of other agencies.

Instead, I urge this Committee to engage with a number of untried and more promising approaches likely to stimulate widespread information security improvements in the private sector. One approach that holds significantly greater promise is the repurposing of SAFETY Act funding toward phased-out information security tax incentives across ten years for small businesses and entrepreneurs. These tax benefits would offer incentives for enterprises that are operating on tight budgets to invest in information security education, hire security personnel, and purchase information security goods and services. A tax incentive approach does not suffer

from the significant negative secondary consequences described above, and it offers a more immediate and direct impact on improving private sector information security.