JULY 28, 2015

PROMOTING AND INCENTIVIZING CYBERSECURITY BEST PRACTICES

UNITED STATES HOUSE OF REPRESENTATIVES, COMMITTEE ON HOMELAND SECURITY

ONE HUNDRED AND FOURTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

COMPILED FROM:

https://homeland.house.gov/hearing/subcommittee-hearing-promoting-and-incentivizing-cybersecurity-best-practices/

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

July 28, 2015

Media Contact: Susan Phalen
(202) 226-8477

Statement of Subcommittee Chairman John Ratcliffe (R-TX)
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

"Promoting and Incentivizing Cybersecurity Best Practices"

Remarks as Prepared

The Subcommittee is meeting today to examine the potential benefits of expanding the Support Anti-Terrorism by Fostering Effective Technologies Act, referred to as the SAFETY Act, to clarify that, on a voluntary basis, cybersecurity products and services can be reviewed and certified to receive enhanced liability protections for large-scale cyber incidents.

Right now, our cyber defenses are weak and because addressing cybersecurity vulnerabilities is costly, we need to find ways to promote and incentivize investment in cybersecurity. We need to incentivize companies to have a robust cyber risk management plan in place.

Through this hearing, we want to hear from our expert witnesses if the SAFETY Act Office at DHS could be leveraged to promote and incentivize cybersecurity best practices within its existing framework. By way of history, the SAFETY Act was part of the Homeland Security Act of 2002, and is a voluntary program that currently provides incentives for the development and deployment of anti-terrorism technologies.

The SAFETY Act ensures that the threat of costly litigation does not deter potential manufacturers or sellers of anti-terrorism technologies, at both small and large companies, from developing and putting into the marketplace products and services that could reduce the risk or mitigate the consequences of a large-scale terrorist event. Companies qualify for the protections afforded by the SAFETY Act by demonstrating, through an ongoing basis, that they have a comprehensive and agile risk management plan. Applicants to this voluntary program must submit to a rigorous and thorough vetting process by DHS' SAFETY Act Office in order to receive liability protections in the event of an act of terrorism.

Homeland security and national security challenges are constantly evolving and the cybersecurity threat is rapidly growing. It is in that capacity that earlier this year we passed HR 1731, the National

Cybersecurity Protection Advancement Act. The goal of that legislation, which passed the House with a bipartisan vote of 355-63 and is now awaiting Senate action, is to strengthen the sharing of cyber threat indicators to guard against criminal groups, hacktivists, or Nation- State actors.

Separately, we have been meeting with stakeholders to find other ways to strengthen cybersecurity, including expanding the SAFETY Act for cyber purposes. Right now the SAFETY Act can only be triggered by an act of terrorism. However, for cyber attacks attribution is extremely difficult to determine. Regardless of whether the hacker was a terrorist, nation state, cyber criminal, or hacktivist, the impact of a devastating cyber attack would be the same. If there is something more that can be done to increase cybersecurity best practices overall, and potentially reduce the likelihood of large-scale cyber attack, this Subcommittee is going to examine it. SAFETY Act coverage for cybersecurity will not solve all our cybersecurity challenges but it has the potential to make a significant improvement in our Nation's cyber defenses.

In the coming weeks, the Committee on Homeland Security will consider House-passed legislation from the 113th Congress that would amend the SAFETY Act to establish a "qualifying cyber incident" threshold to trigger SAFETY Act liability protections for vetted cybersecurity technologies.

The very creation of the Department of Homeland Security stemmed from the attacks on September 11, 2001. While we must and will remain vigilant and do everything we can to prevent another, devastating attack on Americans, we must also recognize that the threat landscape is changing. Cyberspace is in many ways the new frontier, and a "cyber 9/11" is only a matter of time if we fail to strengthen our cyber defenses. So we need to ensure that we are doing everything possible to harden our defenses "left of boom", as they say in military parlance.

This potential legislation has the potential to increase investments in the security and resilience of our Nation's critical infrastructure, including the power grids, air traffic control, and banking systems. Much of our Nation's critical infrastructure is privately owned, and in the 21st century there now exists an interconnectedness of physical security and cybersecurity. This means that someone sitting at a keyboard can now initiate a physical injury by issuing commands to an office building, air traffic control system, or someone's automobile, resulting in loss of life- not just the theft of personal information from a database.

Many products and services weren't built with cybersecurity in mind. This is why we need to incentivize market-driven solutions to raise the bar on how we manage our cybersecurity risks. Fortunately, the United States is home to an ingenious entrepreneurial culture and the best high tech companies in the world who have developed products and services that can help improve the information security resilience of our critical infrastructure and for companies that improve our quality of life.

If amending the SAFETY Act to include "qualifying cyber incidents" would better safeguard our Nation, and potentially prevent a cyber attack that could shut things down and bring commerce to a screeching halt, then we owe it to our constituents to examine the potential benefits it could provide. This is especially true given the increasing importance of cybersecurity in the lives of every American.

###

Brian E. Finch, Esq.

Senior Fellow, The George Washington University Center for Cyber and Homeland Security

July 28, 2015

Hearing on "Effectively Promoting and Incentivizing Cybersecurity Best Practices"

Written Testimony Delivered To The U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Chairman Ratcliffe, Ranking Member Richmond, distinguished Members of the Subcommittee, thank you for inviting me to testify before you today on how to effectively promote and incentivize cybersecurity best practices.

My name is Brian Finch, and I am here today testifying in my capacity as a Senior Fellow with The George Washington University Center for Cyber and Homeland Security, where I am a member of the Center's Cybersecurity Task Force.[1] I am also a partner with the law firm of Pillsbury Winthrop Shaw Pittman LLP, a Senior Advisor to the Homeland Security and Defense Business Council, and a member of the National Center for Spectator Sport Safety and Security's Advisory Board.

Clearly, the implementation of best cybersecurity practices is critical to our nation's economic security and physical safety. Our cyber enemies are numerous, growing, and increasingly sophisticated.

Fortunately there is no lack of will to defend ourselves from the attacks these enemies launch. Unfortunately, given the scale, scope, and pace of cyber threats we face, our cybersecurity measures *writ large* tend to lag behind the said attacks.

[1] While I am testifying in my capacity as a Senior Fellow with The George Washington University Center for Cyber and Homeland Security, please note that my comments represent my personal views and not necessarily any positions of the Center.

In light of those threats, I firmly believe that promoting and incentivizing the use of cybersecurity best practices and effective technologies, policies, and procedures are critical to our nation's security. I also firmly believe that the private sector is ready and willing to adopt those best practices, technologies, policies, and procedures. Its challenge, however, is determining which of those items are in fact "the best" or even "quite good."

Moreover, we should all acknowledge that the private sector will see all of its cybersecurity decisions second-guessed in the tsunami of litigation that inevitably follows any cyber attack. Thus, programs that help companies determine which cybersecurity measures to adopt and will help them minimize their exposure to unnecessarily expensive and protracted litigation are desperately needed.

Thankfully, a program already exists in the United States Code that in fact does promote and incentivize the use of cybersecurity best practices, technologies, policies, and procedures: the "SAFETY Act."

The SAFETY Act, which stands for the Support Anti-Terrorism By Fostering Effective Technologies, was enacted in 2002 as part of the Homeland Security Act. The SAFETY Act is one of the most responsibly designed and effectively implemented liability management programs in government today. More importantly, it can and already has been used to promote improved cybersecurity, and, with the leadership of this Committee, that success can be expanded.

In my testimony below, I will go into greater detail as to how the SAFETY Act can currently be used promote the increased use of cybersecurity practices as well as effective technologies, procedures, and policies. I will also explain why I believe that some very minor statutory tweaks to the SAFETY Act would be exceptionally helpful in expanding its use in the private sector. Finally, I will also provide some examples of how the SAFETY Act could be tied to innovative ideas that will, in general, promote improved cybersecurity.

<u>Important Clarification Regarding the Scope of This Written Testimony</u>

I believe at the outset that it is exceptionally important to establish what I will NOT be promoting in my testimony. I want there to be no misunderstanding with respect to what actions I believe Congress or the Executive branch should be undertaking in order to allow the SAFETY Act to reach its full potential with respect to cybersecurity.

Specifically, my testimony:

- Will NOT advocate for an expansion of the scope of the liability protections offered by the SAFETY Act. The SAFETY Act, as currently drafted, provides to the Department of Homeland Security (DHS) all of the legal authority needed to encourage the widespread deployment of effective and useful cybersecurity technologies, policies, and procedures;

- Will NOT advocate for an expansion of the types of unlawful events that may trigger the liability protections offered by the SAFETY Act. Again, as currently drafted, the SAFETY Act gives the Secretary of Homeland Security broad discretion to decide which unlawful acts that cause harm to U.S. persons, property, or economic interests can trigger its liability protections;

- Will NOT seek to revise or reinterpret the intent of the members of the 107th Congress, who drafted and voted to enact the SAFETY Act;

- Will NOT advocate for the ability of the private sector to excuse itself completely from liability following a cyber attack, much less disincentivize the private sector from continually investing in and upgrading its cyber defenses; and

- Will NOT seek to undermine the ability of DHS to thoroughly review applications for SAFETY Act liability protections or require a dramatic expansion in the size or cost of the Office of SAFETY Act Implementation (OSAI), such that the program office will become unwieldy or unnecessarily costly.

Instead, my testimony will advocate for a very simple proposition: that with the addition of a few well-placed words, it will become perfectly clear to the private sector that the SAFETY Act applies to cybersecurity practices, technologies, procedures, and policies. Moreover, these minor tweaks will permanently clarify that the SAFETY Act applies to cyber attacks committed by a variety of actors, as well as attacks where attribution is unclear or impossible.

<u>The SAFETY Act as Drafted Applies to Cybersecurity Technologies and Cyber Attacks</u>

A critical point that must be established immediately is that both the SAFETY Act statute (see 6 U.S.C. § 441 – 444) and the implementing Final Rule (see 6 CFR § 25) establish that cyber attacks can trigger the law's liability protections and that information technologies (including cyber security systems and services) are eligible to receive SAFETY Act liability protections.

By way of review, please note that the SAFETY Act provides extensive liability protections to entities that are awarded either a "Designation" or a "Certification" as a Qualified Anti-Terrorism Technology (QATT). Under a "Designation" award, successful SAFETY Act applications are entitled to a variety of liability protections, including:

- *All terrorism-related liability claims must be litigated in federal court;*
- *Punitive damages and pre-judgment interest awards are barred;*
- *Compensatory damages are capped at an amount agreed to by both DHS and the applicant;*
- *That damage cap will be equal to a set amount of insurance the applicant must carry, and once that insurance cap is reached no further damages may be awarded in a given year;*
- *A bar on joint and several liability; and*
- *Damages awarded to plaintiffs will be offset by any collateral recoveries they receive (e.g., victims compensation funds, life insurance, etc.)*

Should the applicant be awarded a "Certification" under the SAFETY Act for their QATT, all of the liability protections awarded under a "Designation" are available. In addition, the Seller of a QATT will be entitled to an immediate presumption of dismissal of all third-party liability claims arising out of, or related to, the act of terrorism.

The only way this presumption of immunity can be overcome is to demonstrate that the application contained information that was submitted through fraud or willful misconduct.80 Absent such a showing, the cyber attack-related claims against the defendant will be immediately dismissed.

Additionally, when a company buys or otherwise uses a QATT that has been either SAFETY Act "Designated" or "Certified," that customer is entitled to immediate dismissal of claims associated with the use of the approved technology or service and arising out of, related to, or resulting from a declared act of terrorism.

As the SAFETY Act is currently drafted, in order for its protections to be triggered, the Secretary of Homeland Security must declare that an "act of terrorism" has occurred. The definition of an "act of terrorism" is extremely broad and includes any act that:

(i) is unlawful;
(ii) causes harm to a person, property, or entity, in the United States, or in the case of a domestic United States air carrier or a United States-flag vessel (or a vessel based principally in the United States on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), in or outside the United States; and
(iii) uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.

The Secretary has broad discretion to declare that an event is an "act of terrorism," and once that has been declared, the SAFETY Act statutory protections will be available to the Seller of the QATT and others.

Critically, nothing in the SAFETY Act statute or Final Rule requires that there be a finding of a "terrorist" intent in order for the Secretary to declare that an "act of terrorism" occurred. Indeed, the only discussion of "intent" when defining an "act of terrorism" comes in the third part. There, all Congress drafted was that the attack must have used a weapon or other instrumentality "intended" to cause some form of injury.

Congress had every opportunity to explicitly or implicitly limit qualifying "acts of terrorism" to politically, religiously, or other ideologically motivated actions by specifically defined groups or persons. It chose not to do so, instead stating that, for purposes of the SAFETY Act, an "act of terrorism" was simply an intentional unlawful act intended to cause harm to U.S. persons, property, or economic interests.

It can only follow then that the SAFETY Act statute can (and is) interpreted to include cyber attacks as an act that can be considered an "act of terrorism" and may serve as a trigger for the protections of the SAFETY Act.

Further, it is vital to note that the SAFETY Act Final Rule includes cyber security products and services in its definition of "Qualified Anti-Terrorism Technologies," or "QATT," or technologies that are eligible to receive SAFETY Act protections.

This point is readily demonstrated by the fact that DHS, through its Office of SAFETY Act Implementation, has already approved a number of cyber security products and services. By that measure alone, we know that the SAFETY Act applies to a variety of cyber security products and services.

Still, it is important to understand the statutory and regulatory basis for the coverage of cyber security products and services under the SAFETY Act.

We can start with the SAFETY Act itself, specifically in 6 USC § 444(1), defines a "Qualified anti-terrorism technology" as follows:

> For purposes of this part, the term "qualified anti-terrorism technology" means any product, equipment, service (including support services), device, or technology **(including information technology)** designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, that is designated as such by the Secretary.

(emphasis added).

Note that this definition specifically covers "information technology" and, further, that the only characteristic needed by any product, equipment, service, device, or technology in order to be considered as a QATT is that the item "is designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause."

Thus, by its explicit terms, information technologies – a term that includes cyber security products and services – are eligible to be considered as a QATT under the SAFETY Act.

We should also consider the QATT definition set forth in 6 CFR Part 25.2, which reads as follows:

> *Qualified Anti-Terrorism Technology or QATT*—The term "'Qualified Anti-Terrorism Technology" or "QATT" means any Technology ***(including information technology)*** designed, developed, modified, procured, or sold for the purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, for which a Designation has been issued pursuant to this part.

(emphasis added).

DHS also explicitly refers to information technologies when defining Qualified Anti-Terrorism Technologies and also links "information technologies" to any Technology designed, etc. to combat an "act of terrorism."

Therefore, any Technology designed, developed, modified, procured, or sold for the purpose of preventing, detecting, identifying, or deterring "acts of terrorism" will be eligible to be defined as a QATT. That includes cybersecurity products and services.

I would also refer the Committee to the SAFETY Act Final Rule's definition of "Technology," which is as follows:

> *Technology*—The term "Technology" means any product, equipment, service (including support services), device, or technology ***(including information technology)*** or any combination of the foregoing. Design services, consulting services, engineering services, software development services, software integration services, threat assessments, vulnerability studies, and other analyses ***relevant to homeland security*** may be deemed a Technology under this part.

(emphasis added).

Please note that here again DHS specifically used the term "information technology," once again establishing that cybersecurity products, equipment, or services will be considered a "Technology" for purposes of the SAFETY Act.

Please note too that when elaborating on the types of "design services" that may be considered a "Technology" (a definition that includes various types of software development and support services), DHS stated that "analyses relevant to homeland security may be deemed a Technology under this part." See 26 CFR Part 25.2.

The use of the general term "homeland security" is of great import to this hearing. As this Committee is well aware, DHS's "homeland security" mission is an "all hazards" one, which includes protecting against cyber threats in all forms. Indeed, in recent years the cyber security mission – whether related to terrorist groups, nation-states, organized crime, individuals, or others – has become a primary mission area for DHS. It follows then that when DHS defined "Technologies" for SAFETY Act purposes to include software services related to "homeland security," it intended that term to encompass cyber attacks in their myriad of forms.

In summary, then, there is no question that cyber attacks, regardless of who conducted them or why, and cyber security products and services are eligible to receive SAFETY Act protections under the plain language of the SAFETY Act statute and the Final Rule as originally drafted.

<u>The Nation Would Benefit If Congress Were to Amend the SAFETY Act in a Way That Makes Its Coverage of Cyber-Attacks Cyber Security Technologies Even More Explicit</u>

Despite the fact that the SAFETY Act, as already drafted, encompasses both cybersecurity products and services and cyber attacks unconnected to specific "terrorist" groups or motivations, too many people are unsure of whether the SAFETY Act applies to exactly those items and situations. In short, the only way to rectify the situation is for Congress to slightly amend the SAFETY Act to make explicit its coverage of cyber attacks and cybersecurity products and services.

Thankfully, the path and process for clearing up the SAFETY Act's application in the cyber context has already been blazed, and all this Committee and the House of Representatives need to do is retrace its steps.

In the 113th Congress, members of this Committee, including Chairman McCaul, Ranking Member Thompson, Representative Meehan, and Representative Clarke introduced the National Cybersecurity and Critical Infrastructure Protection Act (NCCIP).

Section 202 of the NCCIP would have slightly altered the SAFETY Act by essentially adding two new terms to the existing law: "cyber incident" and "cybersecurity technologies." These new terms would be inserted after the words "act of terrorism" and "anti-terrorism technologies," respectively, in the existing SAFETY Act law.

The purpose of these new terms was simple and straightforward: make it 100% clear to potential users of the SAFETY Act that the law applies to cybersecurity products and services as well as to cyber attacks that one might not colloquially put in the same category as the terrible events of Sept. 11, 2001 or the Boston Marathon bombings.

These changes were apparently not controversial to this Committee or this Chamber, as HR 3696 passed the House by unanimous voice vote. Unfortunately, due to timing issues that prevented the resolution of some concerns by a few Senators, Section 202 was not included when the final version of HR 3696 passed the Senate and was signed into law. Still, I remind this Committee again that Section 202 was passed unanimously by the House, and so this Committee should pass the SAFETY Act clarifying language once again.

This clarification continues to be absolutely vital for a variety of reasons. First, I can state without qualification to this Committee that the vast majority of eligible SAFETY Act applicants do not realize after reading its statutory language that the SAFETY Act covers non-"terrorist" related cyber attacks or even cybersecurity products and services in general.

Rather, most people who are not steeped in the nuances and history of the SAFETY Act simply see the words "act of terrorism" and "Qualified Anti-Terrorism Technologies" and think only in terms of al-Qaeda, ISIS, right wing militias, and the like.

The statute or Final Rule evidences no such limitations, and, further, there is no legislative history that I am aware of that would definitively limit the application of the SAFETY Act to such groups, their actions, or items designed to deter, defeat, or combat them.

Inclusion of Section 202 language would eliminate that confusion. All parties would now be fully on notice of the application of the SAFETY Act to cyber incidents and cybersecurity

technologies, thus allowing everyone to get on to the business of deciding whether the SAFETY Act is right for them or if the product or service merits the liability protections it offers.

Second, inserting the term "cyber incident" would be of great value to the Executive branch, particularly the Secretary of Homeland Security. Under the SAFETY Act, the decision to declare an incident an "act of terrorism" is assigned to the Secretary of Homeland Security. Thus she or he is the person who decides whether a company that holds a SAFETY Act award may actually assert the defense in federal court. Without that designation, the defenses of the SAFETY Act are not available under the law to the SAFETY Act awardee.

As the past few years have demonstrated, the decision of Executive branch members to declare a particular event an act of terrorism *in any context* is a difficult one. From the shootings at Fort Hood to the cyber attack on Sony Pictures, and even to the recent cyber attack on the U.S. Office of Personnel Management, the Executive branch treads very cautiously when deciding how to describe an incident. Creative terms such as "workplace violence", "cyber vandalism", or even references to a general "security breach" are used instead of the "T" word.

I offer no opinions on the terms used by the Executive branch in those incidents, yet I would dare say we all agree that there is no disagreement on their impact on American lives and our economy. Lives were lost, businesses were crippled, and government programs have been crippled for years to come. It is those *outcomes* – or more specifically preventing or mitigating them – that Congress was focused on when it passed the SAFETY Act in 2002.

That is why adding the term "cyber incident" as defined in Section 202 of NCCIP is a vital tool to give to the Homeland Security Secretary. The Secretary should have the same flexibility to acknowledge the seriousness of a given incident, and, in the case of the SAFETY Act, trigger specific liability protections, without having to utilize a term that may cause a larger than necessary impact. Section 202 thus represents a simple tool with which to wield the SAFETY Act with greater delicacy.

Finally, I must emphasize that the language of Section 202 only *clarifies* the SAFETY Act and is entirely consistent with the original intent of the law. Section 202 *does not expand the SAFETY Act*, as have argued.

When one looks back at the creation, implementation, and use of the SAFETY Act, it has always been clear that the purpose of the law has been to promote the use by the private sector of useful and effective security products and services in order to deter or mitigate massively damaging unlawful events.

The SAFETY Act was designed to help mitigate those events by providing the possibility of limited liability protections following the unlawful "act of terrorism." These liability protections were deemed needed because of concerns about potentially endless litigation following a major attack.

Time has borne out those concerns. The attacks of 9/11 spurred litigation that lasted more than a decade and whose costs ran well into the hundreds of millions of dollars. Similar litigation

arising out of the 1993 World Trade Center attack also lasted for more than a decade, and now every new terrorist incident spurs numerous new lawsuits.

Cyber attacks are no different. High profile attacks spur multiple lawsuits, and indeed the cost of managing litigation post-cyber attack is beginning to represent one of the most expensive consequences of a cyber attack. Considering that millions of cyber attacks occur daily, and that these attacks are growing more sophisticated and successful with each passing moment, liability protections for cybersecurity vendors and users are absolutely critical.

This is especially true given that many of these attacks are conducted by foreign governments and are essentially unstoppable by the private sector. That fact will not deter plaintiffs' counsel, however, and so no matter how good a product is or how much is invested in defensive programs, companies will still face massive litigation. That trend cannot continue, and so it is only proper to use the SAFETY Act as originally intended to control that outrageous trend.

In summary then, clarifying – but not amending – the SAFETY Act so that it explicitly covers cyber incidents and cybersecurity technologies is not only appropriate given the seriousness of the cyber threat. It is also appropriate given the general misunderstanding of how the SAFETY Act works and the need to provide flexibility to the Homeland Security Secretary when determining whether to let the protections of the SAFETY Act be applied.

Optimizing Use Of A Clarified SAFETY Act

Clarifying the SAFETY Act so that it clearly applies to non-"terrorist" cyber-attacks and cybersecurity products and services will have multiple benefits. Please allow me to highlight two examples of improved cyber security this Committee would likely support that would benefit from a clarified SAFETY Act.

1) "Cyber Risk Groups"

One challenge facing private sector companies when implementing cyber defenses is how to effectively cooperate with other companies to protect themselves and best use their limited resources. Particularly using a clarified SAFETY Act, companies could use risk-pooling mechanisms to increase their defenses and better mitigate risk.

Risk pooling mechanisms come in a number of forms, including "risk purchasing" and "risk retention" groups. Those groups allow collections of companies (usually similarly situated in terms of industry sector) to jointly purchase or create insurance coverage that would otherwise be unavailable or excessively expensive.

Here's how it can work:

1. A group of similarly situated companies agree to form a risk purchasing or retention group in order to obtain cyber security insurance.

2. The companies agree to use certain security standards or technologies (for instance SANS 20 controls, "detonation chambers," information sharing via dedicated "private clouds," the recent National Institutes of Standards and Technologies voluntary cyber security framework, etc.)

3. The companies then pool their resources to either jointly purchase an existing cyber insurance policy or to create a pool of insurance that they would maintain.

4. The risk group also agrees to pursue SAFETY Act protections for the standards it has created and committed to adhering to.

5. As part of the agreement, any company that fails to adhere to the security standards will be asked to leave the group at the next renewal period.

Using a clarified SAFETY Act on top of the insurance pool effectively limits the exposure of the group to the amount of insurance they have purchased, or even a portion thereof.

Further, this arrangement also potentially allows more of the insurance funds to be used for losses the company has directly suffered (damaged equipment, lost data, business interruption, etc.) rather than losses suffered by third parties.

The pool arrangement allows companies to collaborate and establish a baseline of security that each would commit to maintaining, all of which fall under the umbrella of a review by DHS. None of this would be possible without a clarified SAFETY Act.

I would add the pooling/risk purchasing agreement would be of particular value to small businesses or ones that serve historically underserved communities. For instance, cooperatives that provide utility services would benefit greatly from this arrangement as it would allow them to provide broader cyber security at reasonable costs to their members. Considering that their members are in historically underserved communities, this would be an excellent public benefit every member of this committee could support.

2) "Cyber HMOs"

A challenge this Committee and others have faced is how to use cyber insurance to promote best cybersecurity practices. That problem remains unsolved, but I contend a clarified SAFETY Act can help the nation better utilize insurance solutions.

First, I start with the proposition that cyber attacks are a constant threat, much more akin to medical claims than property or casualty claims. We know they will occur on a regular basis, and so insurers need to establish an infrastructure that supports constant care over a lifetime.

Following on the health care analogy, cyber insurers should view their policies through the lens of a health insurance model and not a general liability or casualty policy. In my mind, it follows then that cyber insurers should develop cyber policies using a "HMO" model.

Under that model, the insurer's goal will be to promote the "right" kinds of claims – ones that encourage healthy behavior. Yet even with the incentivizing of healthy behavior, inevitably some sort of disease will work its way into the blood stream. The cyber HMO model works well here too as it will support interventional care that prevents minor scratches from developing into a serious infection.

A best case scenario would work out this way: a "cyber HMO" is established, which companies can gain access to by paying monthly premiums along with associated "co-pays," "deductibles," and similar expenses typically associated with a health insurance plan.

That cyber HMO plan would give the insured access to a vast network of cybersecurity vendors and professionals at discounted rates that could be called upon in the event of a problem (the "co-pays" and "co-insurance" equivalents).

The cyber HMO plans would also provide low cost or even free access to basic "cyber hygiene" care, such routine diagnostic examination of information technology systems, perimeter defense systems, and other basic defense systems (the "annual physical" and "low-cost or free vaccine" equivalents).

More "advanced" defense systems could be subject to a higher co-pay and deductible, and companies could even chose to go "out of network" if they want, but they would have to shoulder more of the cost.

The clarified SAFETY Act would help here, too, by helping decide whether a cybersecurity product or service should be "covered" under this insurance model. By encouraging the use of products or services vetted by DHS through the SAFETY Act, the HMO and its policyholders would have greater confidence in the tools they are using to promote cyber health.

The "cyber HMO" is one that actively rewards healthy cyber behavior – a Gordian knot that no carrier has been able to untie yet using traditional insurance models. That's a critical piece of the cybersecurity puzzle, as the challenge has been how to get companies to engage in *effective* cybersecurity, rather than any form of cybersecurity.

Conclusion

Thank you for the opportunity to testify before the Committee today. I will be happy to answer any questions you might have.

Testimony of
Raymond B. Biagini
Partner
Covington & Burling LLP
850 Tenth Street, NW
Washington, DC 20001
rbiagini@cov.com
202.662.5120

Before the House Committee on
Homeland Security's Subcommittee on
Cybersecurity, Infrastructure Protection, and Security Technologies
July 28, 2015

Good afternoon. Thank you, Chairman Ratcliffe, and the members of this Subcommittee, for the opportunity -- indeed privilege -- to speak with you today about this important topic of potentially expanding the U.S. SAFETY Act to provide needed liability protections arising out of "qualifying cyber incidents," as that term is described in the proposed amendment. I support the proposed approach.

I have a particularly keen interest in this topic, and note that I have always been hesitant to engage in activities that might lead to the amendment of the SAFETY Act, because I am the original author of the core liability protection provision of the SAFETY Act. I wrote that provision in June 2002 at the request of some of our law firm's homeland security contractor clients. Together, we examined the legal landscape and homeland security marketplace immediately following the horrific attacks of 9/11 and quickly recognized the need for new legislation to address key public policy needs:

- To stimulate companies, large and small, to research, design, develop and deploy cutting edge anti-terror technology without fear of enterprise-threatening liability suits.

- To stimulate the terror insurance market which had stopped providing terror coverage after the 9/11 attacks.

- To enhance homeland security in the U.S. and abroad.

Guided by these policy considerations, I drafted in June 2002 the "Certification" section (now Section 863(d)(1), (2) and (3)) of what became the U.S. SAFETY Act, passed by Congress in November 2002 as part of the Homeland Security Act. In short, the SAFETY Act is landmark legislation, eliminating or minimizing tort liability for sellers or providers of anti-terror technology ("ATT") approved by U.S. Department of Homeland Security ("DHS") should suits arise in the U.S. after an act of terrorism.

As described more fully below, DHS has awarded SAFETY Act coverage for hundreds of cutting-edge anti-terror products and services since its inception in 2002, thereby satisfying

many of the policy concerns described above. In fact, in many respects, the SAFETY Act has become a homeland security industry "best practice" risk management technique, spurring companies, including small businesses, to research, design, develop and deploy anti-terror technology to protect America without fear of "enterprise-threatening" tort liability should there be another 9/11 terror incident. But given the remarkably rapid expansion over the past several years of increasingly penetrating cyber attacks on key sections of the American economy and government infrastructure, it is time to thoughtfully consider a surgical upgrade of the SAFETY Act so that that law can "catch-up" to the realities of the cyber threat we now face. In short, the proposed legislation recognizes a fundamental principle: the "trigger" of liability protections for a "qualifying cyber attack" should turn not on the identity of the attacker, i.e., is he or she a terrorist, but on the severity of the attack on critical U.S. interests. Moreover, this amendment will begin to requite the public policy concerns that existed in 2002 and exist today -- the need to incentivize companies to further develop cutting edge cyber solutions and to upgrade and enhance their cybersecurity systems; and the need to stimulate the availability of cyber insurance, particularly for key high-value cyber targets in the energy, aviation, electrical, and healthcare industries. These public policy and marketplace dynamics auger for thoughtful consideration of this proposed legislation.

A. Key Features of the SAFETY Act

1. Liability Protections

Should a company obtain SAFETY Act tort protection from DHS, these protections fall into one of two categories:

> Certification -- the highest form of protection -- creates a presumption that the seller of ATT is immediately dismissed from suit unless clear and convincing evidence exists that the seller acted fraudulently or with willful misconduct in submitting data to DHS during the application process. Certification coverage also eliminates punitive damages claims; requires that any suit after an act of terrorism be filed in federal court; and caps the awardee's liability, usually at its terror insurance limits.

Certification coverage is usually awarded by DHS when the applicant's technology has been widely deployed and has a track-record of "proven effectiveness."

The lesser form of SAFETY Act coverage is known as "Designation" coverage and is usually provided when the anti-terror technology has limited actual deployment in the field:

> Designation -- provides all of the protections under Certification coverage except the presumption of dismissal.

Importantly, certification and designation protections apply "up and down" the supply chain, i.e., the awardee's subcontractors, vendors and distributors "derivatively" obtain the same SAFETY Act tort protections as the awardee. But most important, those that buy or deploy SAFETY Act approved technology -- whether they are commercial or government customers -- also are protected derivatively from tort liability arising out of an act of terror.

2. Limits on the Liability Protections

The SAFETY Act's liability protections are triggered only if DHS's Secretary designates a particular incident an "act of terrorism" under the SAFETY Act. "Act of terrorism" is defined as an unlawful act causing harm to a person, property or entity in the U.S., using or attempting to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or instrumentalities of the U.S. The Secretary of DHS will determine on a case-by-case basis whether a particular terrorist attack is covered under the SAFETY Act. This threshold statutory requirement to first designate a particular attack as an "act of terrorism" under the SAFETY Act before the liability protections are applicable is an obvious limitation that may not be necessary or appropriated in considering whether to expand the SAFETY Act to "qualifying cyber incidents."

The SAFETY Act can also apply "extraterritorially," i.e., even if the act of terror occurs outside the U.S., the SAFETY Act can apply to suits filed in the U.S. so long as the "harm," to include financial harm, is suffered by U.S. persons, property, instrumentalities, or entities. And SAFETY Act protections can also apply "retroactively" to cover anti-terror technologies that an applicant has already deployed and which are substantially equivalent to those technologies for which it has obtained coverage.

The SAFETY Act defines "loss" as death, injury or property damage, including business interruption loss. The definition of "anti-terror technologies" includes "any product, equipment, service (including support services), device, or technology (including information technology)" which has a material anti-terror purpose.

Finally, in order to obtain the tort liability protections, an applicant for SAFETY Act coverage must carry terror insurance which will respond to third-party tort liability suits arising out of a covered act of terrorism. The cost of the insurance cannot unreasonably distort the pricing of the anti-terror technology. The terror coverage limits usually become the applicant's ultimate "cap" on liability. In practice, if an applicant does not have terror coverage, the SAFETY Act Office will work with the applicant to find terror coverage at a price that the applicant can afford.

B. The SAFETY Act as Implemented Since 2002

Over the past 13 years, particularly in the last 7-8 years, DHS has vigorously implemented the SAFETY Act, providing coverage to hundreds of companies -- from small businesses to some of the largest corporations in the world -- for the anti-terror products or services they provide in the U.S. and abroad. In fact, the first SAFETY Act award went to a small company, Michael Stapleton Associates, for its bomb-sniffing dog training regimen, its x-ray screening, and bomb detection system.

Representative SAFETY Act awards over the past 13 years include coverage for:

- threat and vulnerability assessment protocols;
- airport baggage handling systems;

- biometrically secured airport identification and access system under the Registered Traveler Program;

- perimeter intrusion detection systems;

- cargo inspection systems deployed at ports and borders;

- physical security guard services;

- secure broadband wireless communications infrastructure and command and control systems;

- lamp-based infrared countermeasure missile-jamming systems;

- anti-IED jamming systems.

In some of these cases, the SAFETY Act Office was able to "expedite" its review and award of coverage by giving weight to the fact that these anti-terror products and services had proven effectiveness through long-term deployments with federal and military customers.

Importantly, DHS has also awarded SAFETY Act coverage to private and quasi-governmental entities for their security protocols, procedures and policies used to determine the nature and scope of security they deploy to protect their own facilities and assets. Specifically,

- a major chemical company obtained coverage for its facility security services, including its vulnerability assessments, cybersecurity, emergency preparedness and response services and its perimeter security, at its facilities that were governed by the Maritime Transportation Security Act;

- the Cincinnati/Northern Kentucky Airport obtained coverage for its security management plan, its operations and training procedures for its airport police, rescue and firefighting personnel, its emergency operations center, and airport security plans;

- the New York/New Jersey Port Authority obtained coverage for the security assessments and design/architectural engineering services incorporating security-related design features at the New Freedom Tower and World Trade Center site;

- the NFL obtained coverage for the stadium security standards and compliance auditing program;

- three large professional sports venues obtained coverage for their security practices and protocols;

- the New York Stock Exchange Security System obtained coverage for its command and control and integration of a multi-layered security system.

These significant awards, as well as the fact that the Federal Acquisition Regulations now require federal agencies issuing homeland security solicitations to first consult with the DHS

SAFETY Act Office to determine if expedited coverage is appropriate, have helped the SAFETY Act toward reaching its full potential.

C. The Proposed Legislation: A Limited But Appropriate Expansion of the SAFETY Act To Cover Qualified Cyber Incidents

1. Current Atmospheric Conditions

The cyber threat to U.S. governmental institutions and critical infrastructure as well as to commercial entities is increasing at an alarming rate. Examples include:

- the recent hack into OPM affecting over 22 million individuals, apparently by China;
- the 2014 attack on JP Morgan involving cyber theft of data belonging to 76 million households, likely by Russia;
- the attack on Sony Pictures, apparently by North Korea;
- the indictment of 5 Chinese military officials for hacking proprietary data held by Westinghouse and U.S. Steel.

Indeed, on July 22, 2014, the 9/11 Commission authors likened the threat of a cyber attack on U.S. critical infrastructure to the terrorist threat before September 11, 2001, calling "the cyber domain as the battlefield of the future." These authors urged legislation to incentivize enhanced cybersecurity. Further, the U.S. has identified cyber attacks as the single greatest threat to national security and at the forefront of the Nation's defense and critical infrastructure, characterizing cyber attackers as undeterred by the threat "we'll shutdown your systems" if you attack ours.

In addition to these policy-level concerns, market dynamics are at work. Many companies are slow to improve their systems to prevent or mitigate against an attack. Cyber insurance for key sectors of the economy, especially critical infrastructure, e.g., health, financial, can be hard to get and expensive, often containing significant exclusions. The U.S. goal to strengthen cybersecurity resilience by having industry voluntarily follow NIST guidelines is progressing slowly. DHS, Commerce and Executive Branch agencies have suggested that tort mitigation legislation may be necessary to stimulate industry to enhance cybersecurity and the insurance industry to increase its footprint in the cyber market.

2. Why Amend the SAFETY Act To Cover Non-Terror Based "Qualifying Cyber Incident?"

There are numerous reasons that a discriminate expansion of the SAFETY Act makes sense as a means to mitigate increasing cyber threats. The first has to do with the inherent characteristics and differences between a cyber versus terrorist attack. In the latter, public ownership and notoriety of who the perpetrator is, remains a distinct goal and desire of those perpetrating a terrorist attack. Also, while their methods of accomplishing the terror attack are usually simple and "low-tech," what matters to the terrorist is that the victims (as well as his competitors) know **WHO** committed the heinous act. By contrast, the cyber attacker prefers to

be cloaked in secret, to act stealthily, not revealing highly-complex methods, sources or signatures, while being able to suddenly and massively disrupt broad technological networks. As such, the proposed SAFETY Act amendment appropriately focuses on whether a qualifying cyber incident causes "material levels of damage" and "severely affects" the U.S., as the "trigger" for coverage, not on whether the attacker can be labeled a "terrorist."

Second, over the past 13 years, pursuit of SAFETY Act coverage has become a "best practice" for companies in the homeland security market, which necessarily requires such companies to demonstrate "proven effectiveness" of their anti-terror products or services. Indeed, DHS already has awarded coverage for certain cyber security solutions and technologies. DHS's focus on "proven effectiveness" will apply equally to cyber solution providers and those companies that are deciding on the quality and scope of their cyber threat protections program. As such, the SAFETY Act should have the salutary benefit of improving the quality of cyber technology and use, thereby hardening networks and enhancing the level of cybersecurity generally throughout the U.S.

Third, as a prerequisite to obtaining SAFETY Act protection, the Act has always required an applicant to maintain terror insurance coverage; the amendment would similarly require an applicant to maintain cyber insurance to obtain the protections. This combination of liability protections and insurance requirements spurred the terror insurance markets to open up and will likely have the same effect on cyber insurance markets, particularly in the highly-vulnerable aviation, health, electric and energy critical infrastructure arenas. Similarly, if SAFETY Act liability protection is provided to those companies providing proven cyber solutions, especially to high-value targeted industries, the insurance markets will likely respond positively because of the layer of immunity and claims-elimination protection afforded to its insureds if they are sued after a "qualifying cyber incident."

Fourth, the procedures for obtaining SAFETY Act coverage have been demonstrated to be reasonably predictable and, when needed, nimble. These procedures include protocols for expediting or "fast-tracking" applications; modifying a coverage award when a company's technology has materially changed; and renewing coverage after an initial award. Companies who fail to update DHS with material changes to their technology or fail to provide the technology or service as outlined to DHS in obtaining SAFETY Act coverage could find themselves without protection should a lawsuit arise.

That said, the challenge for the SAFETY Act Office will be to obtain the necessary resources and expertise to handle an increased number of cyber-based SAFETY Act applications and to be able to nimbly but meaningfully review cyber applications which inherently involve changing technologies and threat environments.

Finally, the proposed legislation does not conflict with the Senate information-sharing and monitoring bills. These bills focus on the important need to enhance a specific critical activity -- the sharing of cyber threat information between and among commercial and governmental entities -- by providing protection for such sharing and monitoring companies from liability arising out of these specific activities. The proposed House legislation is focused on those companies that design, develop and deploy and use cyber solutions, e.g., threat and theft protection; vulnerability assessments; fraud and identity protection, etc. The House legislation is

meant to incentivize a broad swath of providers and users of such cyber technology by providing significant tort protections afforded under the SAFETY Act should a "qualifying cyber incident" occur.

CONCLUSION

The proposed legislation to discriminately expand the SAFETY Act is reasonably calculated to address both policy-based concerns and market dynamics. Its emphasis on the severity and impact of the cyber attack and not on the identity of the attacker as the trigger for protection is appropriate. DHS's continued requirement that a technology -- cyber or otherwise -- have a record of "proven effectiveness" and the statutory requirement to carry cyber insurance, will likely spur higher quality technology and more available insurance. The challenge for the DHS SAFETY Act Office will be to have sufficient qualified resources who can conduct meaningful and timely reviews in an atmosphere of rapidly changing technology and threats. In the end, this amendment, like the original SAFETY Act, should be driven by a common spirit and intent: to take proactive legislative incentivizing steps now -- to avoid a catastrophic debilitating incident involving a major critical infrastructure or economic sector of the U.S. This proposed discriminate amendment of the SAFETY Act is a step in the right direction.

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.

July 28, 2015

The Honorable John Ratcliffe
Chairman
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

The Honorable Cedric Richmond
Ranking Member
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Ratcliffe and Ranking Member Richmond:

On behalf of the American Gas Association (AGA), the Edison Electric Institute (EEI), and the National Rural Electric Cooperative Association (NRECA) we are writing in support of testimony submitted by Brian Finch on the need to clarify the SAFETY Act to ensure that significant cybersecurity incidents are clearly covered under the programs liability protections.

The electric and gas utility industries take cybersecurity threats very seriously. Any statutory clarification would be beneficial if it helps to make more explicit that cyberattacks are covered by the SAFETY Act and that legal defenses will be available to those using its certified cyber security products or processes in the event of a significant cyber-attack. Currently, the SAFETY Act provides that liability protections are available in the case of an "act of terrorism," which is usually interpreted to include a significant cyber-attack. To eliminate any doubt, Congress should make clear that it intends for a significant cyber-attack to be covered. This clarification would likely result in an increase in utilization of the program and adoption of its certified cyber security products or processes.

We appreciate the Subcommittee's continued focus on this important issue. The changes Mr. Finch has suggested are important and we look forward to working with you as legislation to clarify the SAFETY Act moves forward.

American Gas Association

Edison Electric Institute

National Rural Electric Cooperative Association