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.