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.