VENABLE LLP

Webinar Q & A

AUGUST 2014


AUTHORS

**Dismas Locaria**
dlocaria@Venable.com
202.344.8013

**Brian M. Zimmet**
bmzimmet@Venable.com
202.344.4510

**Jason R. Wool**
jrwool@Venable.com
202.344.4511


# Managing Liabilities from Cyber Threats Using the SAFETY Act

## Questions and Answers

### Would it benefit a 3rd party (consultant) creating a program/plan in response to NERC's CIP-014 for utilities to implement to apply for coverage of the plan?

Yes, absolutely. CIP-014 essentially requires certain Transmission Owners and Operators to develop and implement physical security programs for certain stations and substations. The standard was developed in response to actual terrorist attacks on these types of facilities. Because users of a Designated/Certified program would receive total immunity under the Act, it would make good business sense for a consultant or other organization to gain coverage under the Act for a program that others implement specifically to gain the protections of the Act in addition to other benefits. It is worth noting that the question of whether the SAFETY Act would immunize a Registered Entity from NERC penalties if they implemented a SAFETY-Designated/Certified program is unresolved at this time, but the use of such a program would certainly apply with regard to third-party liability in civil suits arising from an Act of Terrorism, or perhaps indirectly in other suits where negligence is asserted.

### Can you elaborate on the incentives beyond the value of lower insurance premiums and legal liability of having the DHS "Stamp of approval?"

The explicit incentives of the SAFETY Act arising from liability stemming from an Act of Terrorism for holders of Designation include:

- Liability cap at a pre-determined insurance level
- Exclusive jurisdiction in federal court
- Consolidation of claims
- No joint and several liability for noneconomic damages
- Bar on noneconomic damages unless plaintiff suffers physical harm
- No punitive damages and prejudgment interest
- Plaintiff's recovery reduced by collateral sources

In addition to the above, for Certification, holders of the protection also enjoy immunity from liability arising from an Act of Terrorism.

The above are the primary benefits of the SAFETY Act, however, an ancillary benefit, in addition to those detailed in your question, include:

- Market differentiation as the protections extend to suppliers/vendors (perhaps lowering the cost of component parts, subservices, etc.), as well as customers, thereby extending them with a tremendous benefit for procuring your technology over competitors without the protection.

- The federal government's review of a technology and a determination that it is indeed effective at what it does could assist the holder of the protection in defending against allegations of failing to meet one's required duty of care and/or negligence.

### Regarding liability cap at predetermined insurance levels: Is this a specific amount based on the application? If so, is there any recourse if OSAI/DHS determination is disputed by the applicant?

Yes, OSAI determines the required insurance level by reviewing company financials and sales data on the technology. The Act is intended to not unduly distort the cost of a technology due to exorbitant insurance costs, thus, a determination that is out of step with the level of insurance a company might hold based on reasonable business judgment can be challenged and lowered if a business case can be made. We've been successful in making such showings in the past.

### Would self-attestation of a cybersecurity program be enough?

No, the application process is very in-depth and one piece of evidence would not be enough. Also, a self-attestation would not be recommended over a third-party audit of some kind. The use of self-assessments is recommended mostly with regard to determining whether an application would be appropriate given an entity's current state of cybersecurity. That said, much of the evidence provided will be a first-party demonstration of capability – much as NERC-regulated entities are responsible for demonstrating compliance with the CIP Reliability Standards. But again, third-party audits/assessments would be given additional weight due to their stronger inclination towards objectivity.

### How do you reconcile the proposed legislation adding "qualified cyber incident" to the SA with the view that the SA already covers such events?

The current Act with the proposed legislation can be reconciled because currently, the SAFETY Act only covers cyber incidents to the extent they qualify as an Act of Terrorism. This means that they meet the three part definition of an Act of Terrorism. Alternatively, the legislation that recently passed the house defines "qualified cyber incidents" more broadly than just Act of Terrorism. Therefore, such incidents could include cyber events that are not Act of Terrorism, but rather incidents that may have been caused by criminals, hacktivists, etc.

### Are you aware of any cases of SAFETY act application?

To date, the protections of the SAFETY Act have yet to be invoked by any holder of the protection.

### Is this Safety Act implemented as an incentive in direct response to the Cyber EO which required certain government departments to consider what incentives they could offer to those who adopted the cyber framework?

No, the SAFETY Act stems from the Homeland Security Act of 2002 in response to 9/11. The Act is intended to encourage the development and deployment of anti-terrorism technologies by creating systems of "risk" and "litigation management."

## What might be an example of a Service and a Program that you have seen?

To date, there have been approximately 1,000 technologies that have received one of the three SAFETY Act protections. Public information on each of these can be found at: https://www.safetyact.gov/jsp/award/samsApprovedAwards.do?action=SearchApprovedAwardsPublic

Venable office locations


BALTIMORE, MD
750 E. PRATT STREET
SUITE 900
BALTIMORE, MD 21201
**t** 410.244.7400
**f** 410.244.7742

LOS ANGELES, CA
2049 CENTURY PARK EAST
SUITE 2100
LOS ANGELES, CA 90067
**t** 310.229.9900
**f** 310.229.9901

NEW YORK, NY
ROCKEFELLER CENTER
1270 AVENUE OF THE AMERICAS
25TH FLOOR
NEW YORK, NY 10020
**t** 212.307.5500
**f** 212.307.5598

ROCKVILLE, MD
ONE CHURCH STREET
FIFTH FLOOR
ROCKVILLE, MD 20850
**t** 301.217.5600
**f** 301.217.5617

SAN FRANCISCO, CA
SPEAR TOWER, 40TH FLOOR
ONE MARKET PLAZA
1 MARKET STREET
SAN FRANCISCO, CA 94105
**t** 415.653.3750
**f** 415.653.3755

TOWSON, MD
210 W. PENNSYLVANIA AVE.
SUITE 500
TOWSON, MD 21204
**t** 410.494.6200
**f** 410.821.0147

TYSONS CORNER, VA
8010 TOWERS CRESCENT DRIVE
SUITE 300
VIENNA, VA 22182
**t** 703.760.1600
**f** 703.821.8949

WASHINGTON, DC
575 7TH STREET NW
WASHINGTON, DC 20004
**t** 202.344.4000
**f** 202.344.8300

WILMINGTON, DE
1201 NORTH MARKET STREET
SUITE 1400
WILMINGTON, DE 19801
**t** 302.298.3535
**f** 302.298.3550