VENABLE® LLP

Managing Liabilities from Cyber Threats Using the SAFETY Act

Brian Zimmet
Dismas Locaria
Jason Wool

August 5, 2014

VENABLE® LLP

Agenda

1. Introduction
2. The SAFETY Act – An Overview
3. Applicability of SAFETY Act to Cybersecurity Programs

VENABLE LLP

Introduction

- In recent years, increased governmental focus on cybersecurity
  - Computer networks help run everything from the electric grid to bank transactions to air traffic control
  - Government lacks direct control over most networks; thus, the focus on regulating cybersecurity practices
- Certain industries (*e.g.*, electric utilities) subject to mandatory federal cybersecurity regulation
- Executive Order 13636 (issued in 2013) aimed at improving cybersecurity practices in other industries not subject to cybersecurity regulation
- NIST Cybersecurity Framework issued in early 2014

VENABLE LLP

Liability Risks

- Failure of a company to secure/defend adequately its computer networks gives rise to liability risks
  - Tort and breach of contract claims
  - Increased risk of regulation
- Standards of care becoming easier to define with increased governmental attention to cybersecurity practices
- The SAFETY Act can be used to cover a company's internal cybersecurity program, and thus manage these liability risks

VENABLE LLP

The SAFETY Act

- The SAFETY Act (Support Anti-Terrorism by Fostering Effective Technologies Act)
  - Enacted as part of the Homeland Security Act of 2002, Public Law 107-296 (Title VIII, Subtitle G, Secs. 861-65)
  - Implementing regulation at 6 C.F.R. Part 25
- Intended to encourage the development and deployment of anti-terrorism technologies by creating systems of "risk" and "litigation management"
- Technologies include:
  - Products, devices, equipment
  - Services – both supporting and stand-alone services
  - Cyber-related items
    - Information technologies and networks
    - Integrated systems

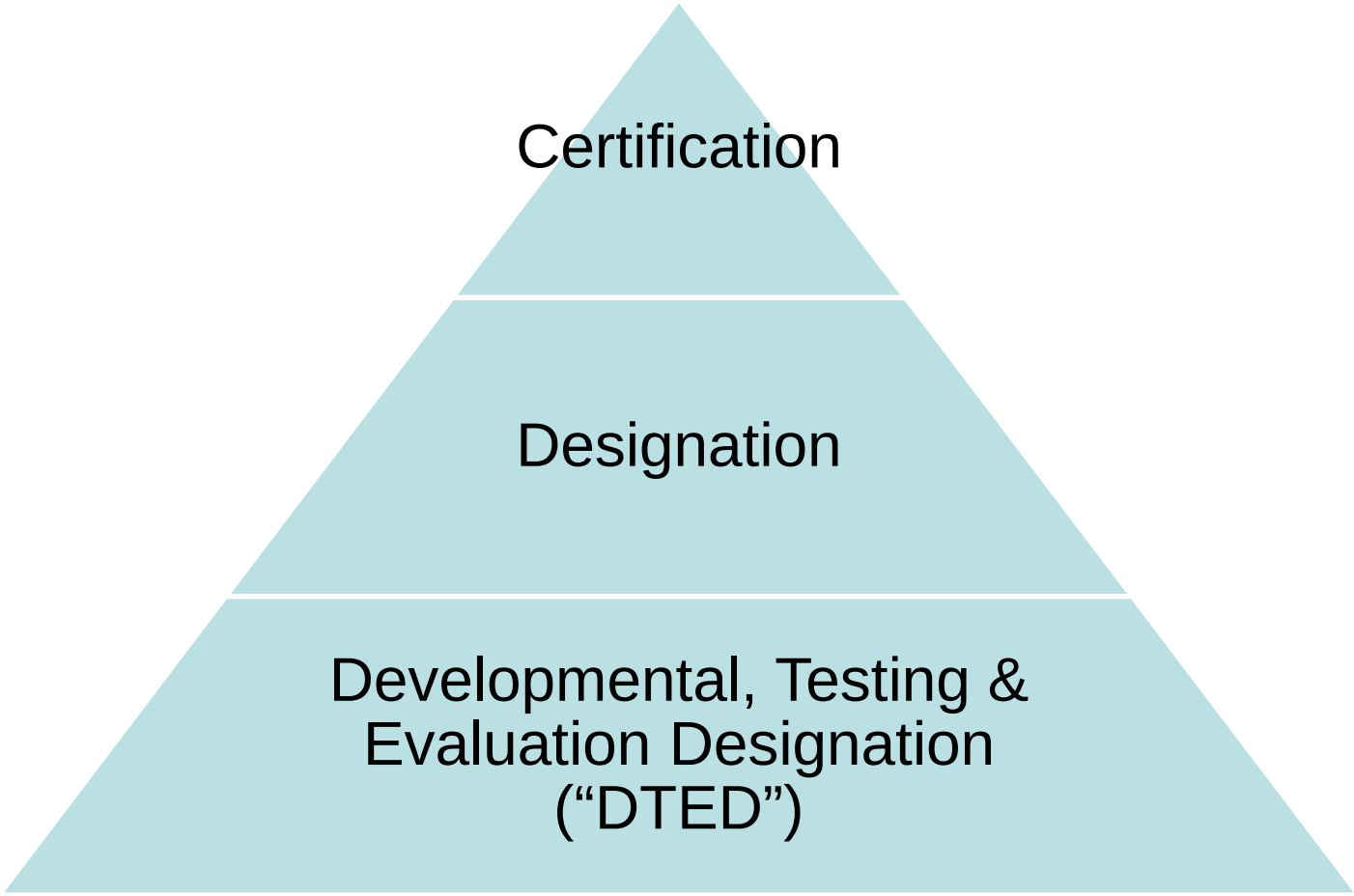
VENABLE LLP

Scope of the Act

- Applies to an "act of terrorism," which may include cyber terrorism
- An "act of terrorism" is defined by DHS as:
  - Unlawful
  - Causes harm, including financial harm, to a person, property or entity, in the United States…; and
  - 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
- Includes attacks committed by domestic terrorists
- May include attacks on foreign soil, if harm is to a person, property or entity in the United States

VENABLE® LLP

Levels of SAFETY Act Protection



VENABLE LLP

Benefits of SAFETY Act Protections

Certification	- All the benefits of Designation - Government Contractor Defense - Typically 5 years
Designation	- 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 - Typically 5 years
DTED	- Same as Designation, but for a shorter duration (typically 3 years) - Typically limited to specific deployments

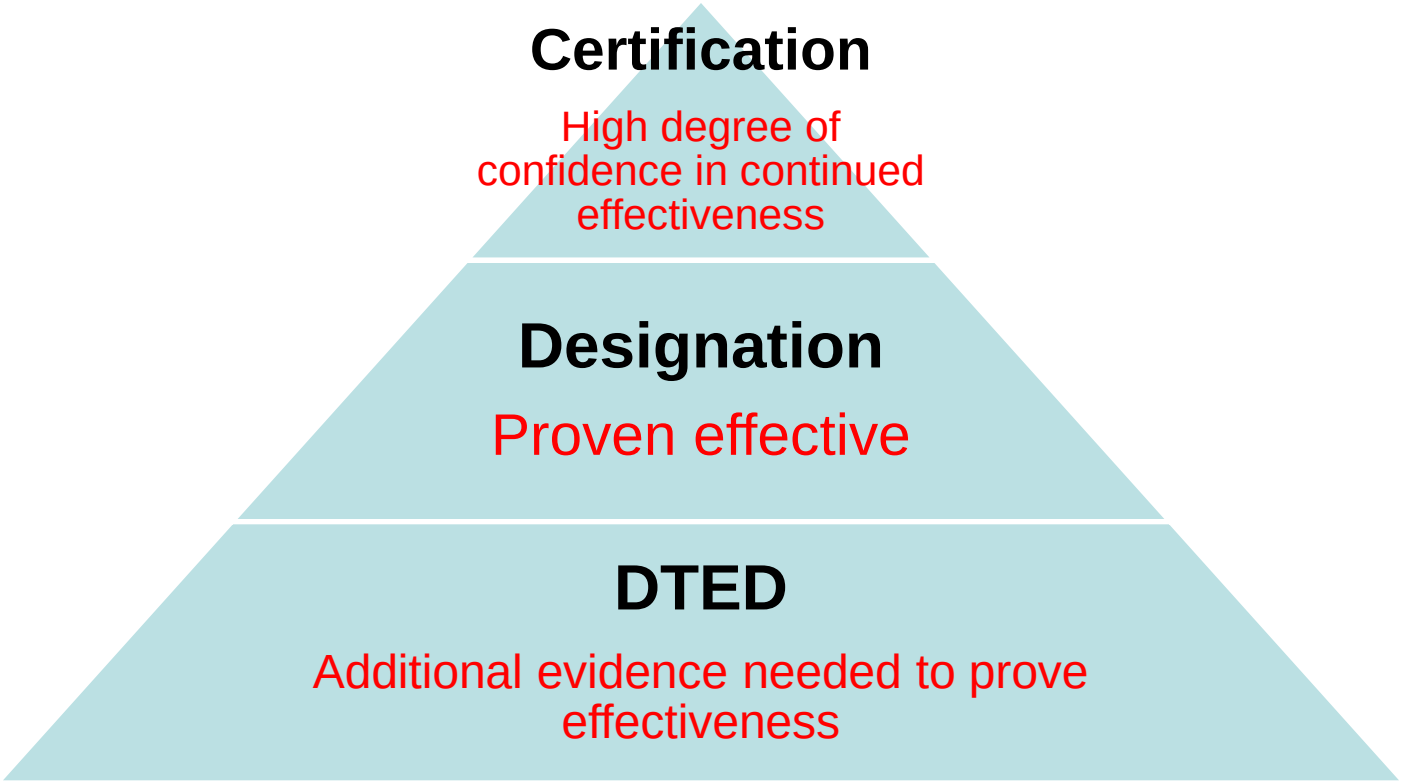
VENABLE® LLP

Criteria for SAFETY Act Protections

Designation (Some not applicable to DTED)	Certification
Prior U.S. Government use or demonstrated substantial utility and effectiveness	Satisfy all the criteria of Designation
Availability for immediate deployment in public and private settings	Perform as intended
Existence of extraordinarily large or extraordinarily unquantifiable potential third-party liability risk exposure to the Seller or other providers	Conform to specifications
Substantial likelihood that the product/service will not be deployed unless protections under the system of risk management provided under the SAFETY Act are extended	Is safe for use as intended
Magnitude of risk exposure to the public if such product/service is not deployed	
Evaluation of all scientific studies that can be feasibly conducted in order to assess the capability of the technology to substantially reduce risks of harm	
The product/service is effective in facilitating the defense against acts of terrorism, including technologies that prevent, defeat or respond to such acts	

Criteria for SAFETY Act Protections *cont'd*

In sum:



Obtaining SAFETY Act Protections

- Pre-application process (optional)
  - For those seeking OSAI guidance on applicability, likelihood of success based on proposed standards, data, etc.
  - 21-day review
- Standard application process:

VENABLE® LLP

The Application Process

Generally requires information and an understanding of the following:

All Applications	Products	Services	Programs

- Register with OSAI
- Points of contact
  - Administrative
  - Subject matter
  - Financial/ insurance
- Customer references
- Description of technology
- Safety issues
- Insurance information
- Financial/sales data
	- Product, components, subcomponents
	- Selection of component manufacturers
	- Manufacturing process, including quality control measures
	- Deployment strategy (does it include maintenance services, lease v. sale)
		- Recruitment and hiring practices
		- Training practices (including initial and recurrent training)
		- Operational policies and procedures
		- Quality control/assurance efforts
		- Selection of subcontractors, if any
			- Development process
			- Baseline standards
			- Implementation of program, including both documentation and actual roll-out
			- Oversight of adherence to program

Additional documentation, enhancements, etc. are sometimes necessary

Submitting an Application

- Once submitted, OSAI/DHS has 120 days to review

OSAI/DHS's Process

- During this timeframe, OSAI will frequently issue questions and requests for additional information
  - Typically 7 to 10 days to respond
  - Does not extend the 120-day clock

VENABLE LLP

Legislative Update

- National Cybersecurity and Critical Infrastructure Protection Act of 2013 passed House on 7/28
- Among other features, amends the SAFETY Act to add “Qualifying Cyber Incident” as a trigger for protections in addition to an Act of Terrorism
- Remains to be seen if a companion bill will/could pass the Senate or if President would sign

VENABLE LLP

SAFETY Act Coverage of Physical and Cyber Security Plans

- SAFETY Act covers products and services that a seller provides to others *and* itself, *i.e.*, its own physical and cybersecurity programs
- Covered entities are encouraged to base their programs on accepted standards, particularly in the cyber context, in order to:
  - Provide a baseline against which practices can be compared for purposes of application
  - Corroborate that the plan is effective and otherwise reasonable

VENABLE® LLP

Choosing the Right Standard

- There is no set standard that must be used to be Designated or Certified technologies
  - OSAI is currently working to develop a standard methodology for review of cybersecurity applications
- Entities generally have an array of guidelines, standards and frameworks from which to choose
  - Main criteria is reputation and wide level of acceptance
  - Some popular examples: NIST SP800-53, ISO 27001, COBIT 5, Top 20 Critical Controls

VENABLE® LLP

Regulations as a Standard

- Using regulations as a standard is possible but requires additional showing
- Compliance with regulatory obligations, on its own, is not sufficient to gain coverage under Act
- Regulations can still be used as the basis, but the service must be “regulations +” to be accepted
- May be able to use regulations to gain protection for systems/assets not subject to regulation (*e.g.*, electric distribution assets)

VENABLE® LLP

What Is OSAI Looking For?

- Whatever standards you choose, recommended that you (and counsel) approach OSAI before applying to receive feedback on proposal
- Looking for programs that
  - Are top or close to top of given industry
  - Demonstrate strong commitment to security
  - Manifest substantial investment in security
  - Demonstrate significant programmatic maturity (strong controls, continuous improvement, sophisticated capabilities, etc.)

VENABLE® LLP

Examples of SAFETY Act Protections for Cybersecurity and Security Programs

American Chemistry Council, Inc. ("ACC")

January 29, 2014 - The American Chemistry Council, Inc. ("ACC") provides The Responsible Care® Security Code (the "Technology"). The Technology consists of a security management system encompassing 13 management practices. The Technology enhances the ability of ACC member and Partner companies to deter, detect, delay, defeat or respond to a physical or cyber attack against any form of chemical operation, whether at a fixed facility or during transportation. This Designation will expire on January 31, 2019.

Bank of America Corporation

March 08, 2013 - Bank of America Corporation provides its Critical Infrastructure Protection and Security Services to protect and secure critical infrastructure and to keep safe customers, employees, contractors and visitors at Bank of America facilities. The Technology is an integrated security system consisting of policies, procedures, services and component systems designed to provide a centralized capability to assess changing threat conditions and activities which could pose a threat to the bank's enterprise and to take actions to mitigate and respond to such risks. The Technology includes services performed by Bank of America Corporation's Protective Services Group and Security Operations Analysis and Command Center ("SOACC"). This Designation and Certification will expire on March 31, 2018.

VENABLE LLP

The NIST Cybersecurity Framework

- Implementation of the NIST Cybersecurity Framework is highly encouraged as part of the program sought to be covered
  - Developed for CI per direction of EO 13636
  - C-Cubed managed by DHS
  - Emphasizes enterprise risk management in addition to desired outcomes in Core
  - Flexible and scalable
  - Relies on existing standards, guidelines and other resources to achieve desired security outcomes
  - Useful for self-assessment
  - Maturity indicators built in (Tiers)

VENABLE® LLP

How We Can Help

- Phase I: Program Assessment/Improvement
  - Review current evidence/interview SMEs
  - Assess maturity, compliance with chosen standard, identify potential gaps vis-à-vis chosen standard(s)
  - Recommend changes that would better support application
  - Privileged and confidential
- Phase II: Consultation with OSAI
  - Confidentially approach, present facts, identify any concerns
- Phase III: Complete Application

VENABLE LLP

SAFETY Coverage Makes Business Sense

- Even in the absence of an act of terrorism, the SAFETY Act provides numerous benefits:
  - Lower insurance premiums
  - Government approval of security program can serve as a defense against lawsuits
  - Government seal of approval can be a boon in the marketplace
- By purchasing SAFETY-covered technologies/services, entities can also receive additional liability protections

VENABLE® LLP

Questions?

VENABLE® LLP

Contact Us

Brian M. Zimmet
bmzimmet@Venable.com
202.344.4510

Dismas Locaria
dlocaria@Venable.com
202.344.8013

Jason R. Wool
jrwool@Venable.com
202.344.4511