VENABLE® LLP

Liability Management – Evolving Cyber and Physical Security Standards and the SAFETY Act

JULY 17, 2014

VENABLE® LLP

Agenda

1. Security Risks affecting the Maritime Transportation System (MTS)
2. The SAFETY Act as an effective risk management tool
3. SAFETY Act coverage for physical security and cybersecurity practices
4. Questions

VENABLE® LLP

Importance of U.S. Ports to National Security and Economy

"Ports, waterways and vessels handle billions of dollars in cargo annually, and an attack on our nation's marine transportation system could have dire consequences. Ports are inherently vulnerable to terrorist attacks because of their size, general proximity to metropolitan areas, the volume of cargo being processed, and the ready access the ports have to transportation links into the United States. An attack on a large port could also have a widespread impact on the broader global supply chain . . . and the world economy."

Statement of Stephen L. Caldwell
Director, Homeland Security and Justice
Before the Committee on Homeland Security
and Governmental Affairs, U.S. Senate
June 4, 2014

VENABLE® LLP

Security Risks affecting the MTS

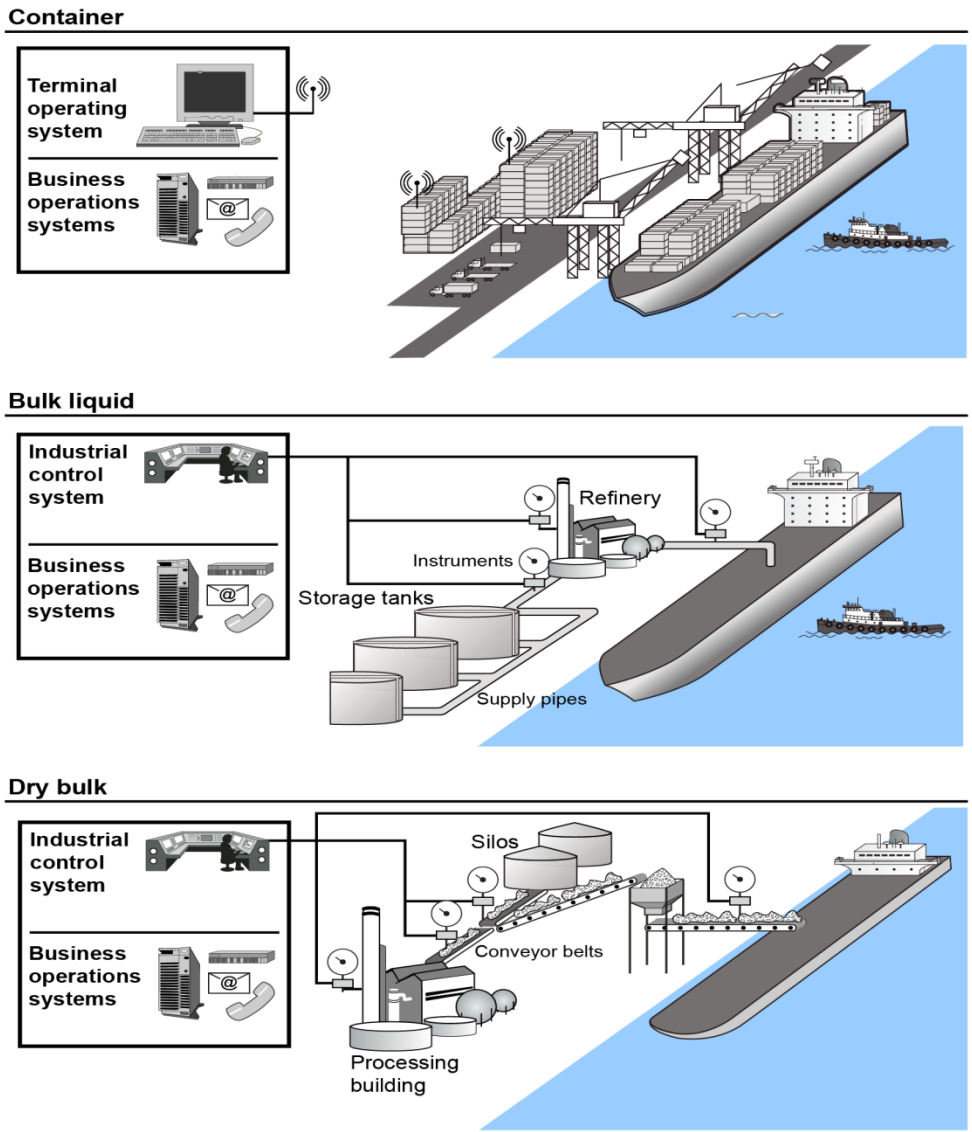
- Physical security risks are well-documented (terrorist attacks on ports and vessels, piracy, etc.)
- Cyber-risks are less understood but are increasing in frequency and severity
  - MTS is not currently subject to mandatory cybersecurity regulation, but increased regulation could be imminent
  - Area, vessel, and facility security assessments all currently require consideration of radio and telecommunication systems, including computer systems and networks. This could become more prescriptive under the Maritime Transportation Security Act (MTSA)

VENABLE LLP

IT Dependency Leads to Potential Vulnerability

- Per GAO, port owners and operators rely on several forms of information and communications systems to operate
  - Terminal Operating Systems
  - Industrial Control Systems (ICS)
  - Business Operations Systems
  - Access Control and Monitoring Systems
- Vessels rely on technologies such as GPS, marine Automatic Identification System (AIS), and Electronic Chart Display and Information System (ECDIS)
- These technologies are not always secure and can lead to attacks and compromises.

Examples of Technologies Used in Maritime Ports



System descriptions

Terminal operating systems

Control container movement and storage in the maritime port, among other things. Examples of data that terminal operating systems could contain include shipping information, cargo categorization, and records of container movement.

Business operations systems

Support the business operations of the terminal, such as communication with customers and preparation of invoices and billing documentation.

Industrial control systems

Facilitate the movement and processing of goods throughout the terminal, including the operation of motors, pumps, valves, signals, lighting, and access controls.

Source: GAO analysis of maritime sector information; Art Explosion (clip art).

VENABLE® LLP

Cyber Vulnerabilities Are Not Well Understood

- A 2013 Brookings report found that only 1 of 6 ports reviewed had conducted vulnerability assessments; none had an incident response plan.
- GAO reports that area maritime security plans (AMSPs) and facility security plans (FSPs) reviewed provided only limited consideration of cyber-risks
  - Guidance for developing AMSPs and FSPs to be updated in 2014 to require “basic” considerations of cyber issues

VENABLE LLP

The Cyber Threat is Real

- Per DHS, “the severity of cyber-related threats has only recently been recognized”
- Actual attacks show that cyber-attacks are not merely hypothetical
  - Antwerp port hack
  - Oil rig attacks
  - Attacks on ships facilitated by data resulting from hack
- Known vulnerabilities in ICS, GPS, AIS, and ECDIS could soon be exploited by threat actors (terrorists, organized crime, hacktivists, etc.)

VENABLE® LLP

Port of Antwerp – A Case Study

- From 2011 to 2013, drug traffickers concealed an unknown quantity of heroin and cocaine with street value of over $210 million inside shipping containers
- Traffickers recruited computer hackers to infiltrate IT systems at Port of Antwerp that controlled the movement and location of containers
- Hackers e-mailed malware to staff at the Port that enabled hackers to get remote access; when malware discovered and removed, traffickers broke into offices and installed data interception hardware and key loggers
- Armed with this information, traffickers located the containers, sent in drivers to pick them up, and erased the data to cover their actions

VENABLE® LLP

Stakes Are High

- Economic impact of a successful attack could be substantial.
  - Per GAO, U.S. maritime ports handle more than $1.3 trillion in cargo annually
  - Cyber attacks against oil and gas infrastructure alone will cost energy companies close to $1.9 billion by 2018
- Some attacks could also result in loss of life and/or environmental catastrophe

VENABLE LLP

Why Worry About Cyber in the Absence of Explicit Regulation?

- Lawsuits
  - Negligence
  - Breach of contract
  - Shareholder
- Regulatory enforcement actions
- Criminal actions
- Share price considerations for public companies
- Not to mention first party costs to contain reputational harm, etc.

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

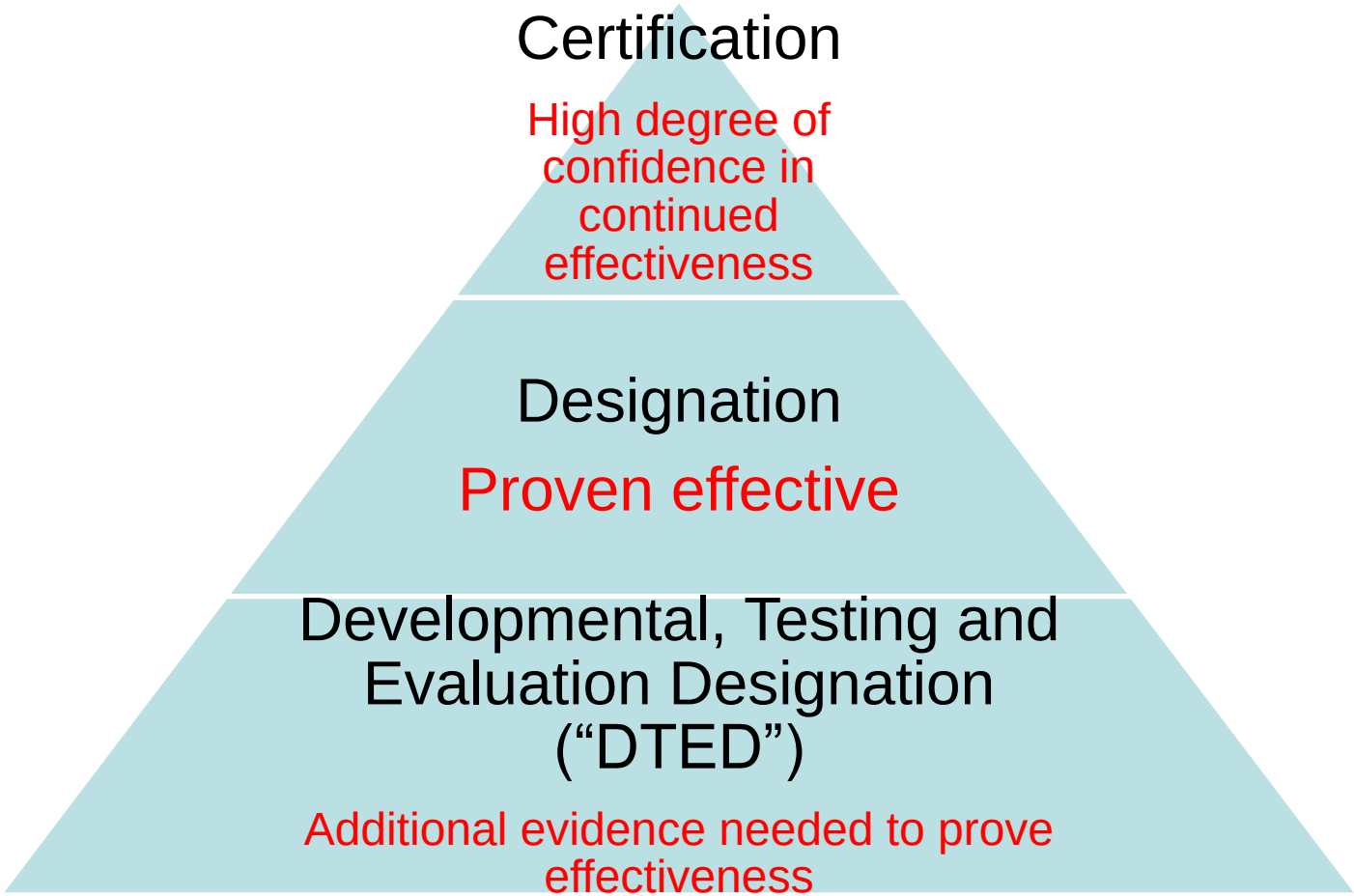
VENABLE® LLP

Scope of the Act

- Applies to an “act of terrorism,” which is 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

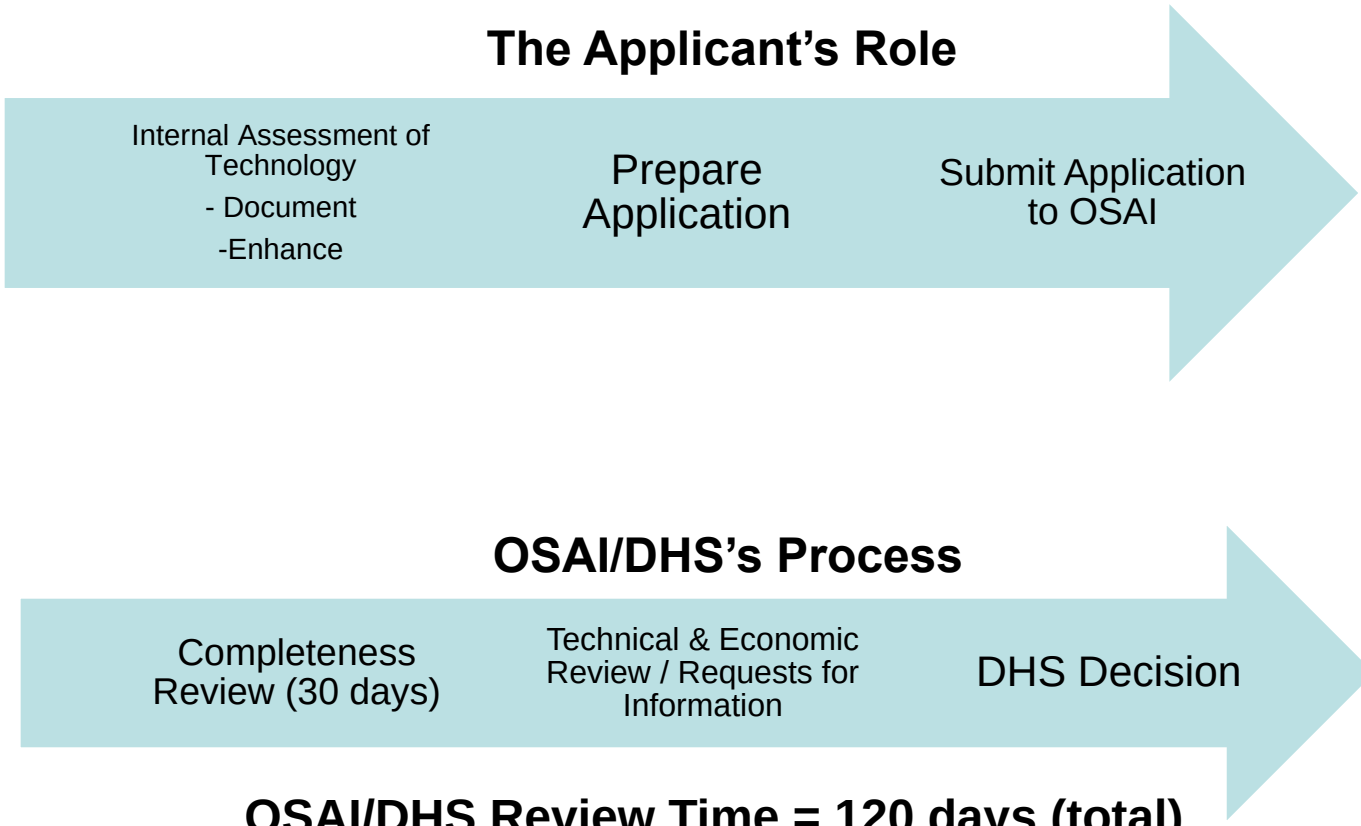


VENABLE® LLP

Benefits of Protections

Certification	- All the benefits of Designation - Government Contractor Defense
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
DTED	- Same as Designation, but for a shorter duration (3 yrs)

Obtaining SAFETY Act Protections



OSAI/DHS Review Time = 120 days (total)

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

- In most instances, entities will have an array of guidelines, standards, and frameworks from which to choose.
  - Main criteria is reputation and wide level of acceptance
  - Often indicated by ANSI accreditation, propagation by trusted sources, etc.
  - In some cases, regulations may be used as the basis for a program

VENABLE LLP

The NIST Cybersecurity Framework

- In the cyber context, implementation of the NIST Cybersecurity Framework is highly encouraged as part of the program sought to be covered by the SAFETY Act.
  - Developed per direction of EO 13636
  - Emphasizes risk management
  - Flexible and scalable
  - Relies on existing standards, guidelines and other resources to achieve desired security outcomes.

VENABLE LLP

The Framework is a Good Fit for MTS

- OSAI is part of DHS, which is responsible for the voluntary program associated with Framework (C-Cubed)
- Coast Guard “strongly encourages” review of Framework in ALCOAST 122/14 and is seeking feedback on its applicability to the MTS.
- FEMA’s 2014 Port Security Grant Program guidance encourages applicants to propose projects to assist in implementing Framework

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
  - Gov. approval of security program can serve as a defense against lawsuits
  - Gov. 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?