AAPA

Port Administration & Legal Issues Seminar
April 15 - 17, 2009
Baltimore

Panel Presentation on Security

Friday, April 17, 2009
8:30 am – 9:45 am

Panel Moderator:	**Thomas G. Schroeter**
Panelists:	**Steven Roberts**
	Brian Finch

Panelist Bios

THOMAS G. SCHROETER

- Thomas G. Schroeter, a member of the State Bar of Texas since 1983, has been Associate General Counsel of the Port of Houston Authority since 2001 where he spends a substantial portion of his attorney time on security matters.

- He is Vice Chairman of the Law Review Committee of the American Association of Port Authorities (AAPA).

- He is a member of the Houston-Galveston Area Maritime Security Counsel's (AMSC's) TWIC Subcommittee and also sits as an advisor to the Houston Ship Channel Security District's Advocacy Committee.

- Mr. Schroeter is a member of the Port of Houston Authority's Senior Management Review Committee for the Authority's ISO 28000-certified Security Management System (SMS), the first port so certified.

- He has been a frequent speaker on security issues in national and local conferences, including conferences of the AAPA.

- Mr. Schroeter is a graduate of Georgetown Law Center in Washington, D.C. where he was an Editor of the Georgetown Law Journal.

Panelist Bios

Steve Roberts

- Steve Roberts is an attorney who practices in the rapidly developing area of homeland security law and regulation. He is currently a columnist for the National Law Journal and for Chemical Week, where he writes on homeland security regulation, with a special emphasis on the Chemical Facility Anti-Terrorism Standards (CFATS), rail transportation security, the Transportation Worker Identification Credential (TWIC), and critical infrastructure related public policy.

- Steve's work in homeland security and counterterrorism began in 1999 and he is a regular guest instructor at the United States Department of Homeland Security's Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia, and the Air Force Special Operations School at Hurlburt Field, Florida. He is also an Adjunct Professor of Law at the University of Houston Law Center.

- Steve is a member of the Florida Bar and the Bar of the District of Columbia and received his undergraduate degree, Cum Laude, from the School of Foreign Service at Georgetown University and his law degree, Magna Cum Laude and Order of the Coif, from the University of Florida.

Panelist Bios

Brian E. Finch

- **Brian Finch joined Dickstein Shapiro in 2006, as counsel in the Government Law & Strategy Group and head of the firm's Homeland Security Practice. Mr. Finch focuses his practice on homeland security, Federal regulatory matters, and government affairs. He is recognized as an authority on homeland security matters, and has counseled numerous clients extensively on matters related to Department of Homeland Security regulations and guidelines, as well as those promulgated by other Federal agencies.**

- **Particular areas of focus for Mr. Finch include the SAFETY Act, protection of critical infrastructure, state and local grant funds, interoperable communications, bioterrorism, food and agricultural security, and border and trade security.**

- **Prior to joining Dickstein Shapiro, Mr. Finch was an attorney with a Washington, DC law firm and worked as a legal intern with the Office of Chief Counsel of the Drug Enforcement Administration, U.S. Department of Justice.**

- **Mr. Finch received his B.S. from Cornell University, his M.A. from The George Washington University's Elliott School of International Affairs, and his J.D. from The George Washington University School of Law.**

Port of Houston Authority

TWIC now required for unescorted access to secure areas of U.S. ports

TWIC Dashboard (Page 1 of 3)
April 9, 2009

Explanation of Dashboard

The TWIC Dashboard provides point-in-time program information on:

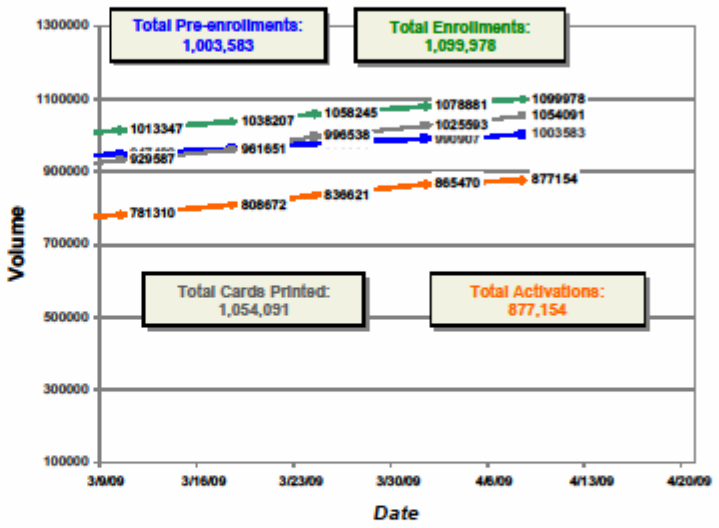
- Enrollment and adjudication-related statistics
- Graph depicting pre-enrollment, enrollment, cards printed & activated trends
- Contact information for TWIC resources
- Total enrollments and activations by location (including total enrollments broken out by occupation type).

Program Statistics

Enrollment/Activation	Measurement (as of 04/08/09)
Pre-Enrollments	1,003,583
Enrollments	1,099,978
Cards Printed	1,054,091
Cards Activated	877,154
Average Enrollment Time	8.83

Security Threat Assessment	Measurement (as of 04/05/09)
Initial Disqualification Letters	37,944
Appeals Requested	20,205
Appeals Granted	18,201
Waivers Requested	3,136
Waivers Granted	1,476
ALJ Review Requested/Granted	11
Final Disqualification Letters	164
Number of Expired IDTAs	10,356

Enrollment Trending



TWIC Information and Resources

Help Desk: 1-866-DHS-TWIC (1-866-347-8942)
8:00 AM ET - 12:00 AM ET
http://twicinformation.tsa.dhs.gov/twicinfo/contact.jsp

Website: www.tsa.gov/twic

Pre-9/11: Traditional Law Enforcement: Concerns about Theft, Drug Smuggling

After 9/11: Concern about WMDs Entering U.S. at Our Seaports in Containers

1993 World Trade Center Bombing: One Month after Clinton Inauguration

World Trade Center after February 1993 parking garage bombing

September 11, 2001 Attacks:
Eight Months after Bush Inauguration

September 11, 2001 World Trade Center attack

Three Months after Obama Inauguration:
North Korea - Rocket Test.
Somalia - Piracy Crisis.

What is Next?

Department of Homeland Security's Agencies Dealing with Maritime Security

Who is Responsible for What in Maritime Security

1. Security on the Water

2. Cargo and Container Inspections and Security

3. Facility (Landside) Security- Access Control per Applicable Regulations

"Top Ten"
Take Home Pointers

1. Who's Who in Your Port in Maritime Security
2. Main Sources of Maritime Security Law & Regulation
3. Facility Security Assessment (FSA) and Facility Security Plan (FSP)
4. Insurance & Risk Resources
5. What Security Measures Are in Your Contracts and Leases?
6. Sensitive Security Information - SSI
7. Port Security Grant Program (PSGP)
8. Your Port is Unique – What are the Real Threats?
9. Learn More and Stay Abreast of Developments in Maritime Security
    a. MARSEC Levels
    b. Emergency Response Plans
    c. Equivalency Security Measures 33 CFR § 101.130
    d. ISO's Security Management System (SMS)
    e. Regional Partnerships; Sharing Agreements; Houston Ship Channel Security District (HSCSD)
    f. Laws and Initiatives to Secure Global Commerce, RPMs, CT-PAT, CSI, new "10-2" rules; 100% Cargo Screening – Pros and Cons
10. You Can Make a Difference!

Take Home Pointers

1. WHO'S WHO

- Get to know your security departments and their managers and Facility Security Officers (FSOs).
- Make an effort to meet the U.S. Coast Guard Captain of the Port and his/her security specialists in Facility Security Plans, TWIC and Emergency Response.
- See if you can attend meetings of the Area Maritime Security Committee, and volunteer to work for one of its subcommittees on TWIC, Grants, or other area involving port security.
- Meet the Customs officer in charge of your port facility and talk to him or her about what Customs does at your port. There is much you can do to assist them and benefit your ports.

Take Home Pointers

2. Main Sources of Maritime Security Law

- The Maritime Transportation Security Act of 2002
- The SAFE Port Act of 2006 (a/k/a The Security and Accountability For Every Port Act of 2006).
- Regulations promulgated under MTSA and the SAFE Ports Act, primarily in 33 CFR, Parts I-V, and 49 CFR Part 1572.
- The TWIC Final Rule, published in the Federal Register on January 25, 2007, and incorporated in the CFR Regulations in 33 CFR Parts 1 and 5: 49 CFR Part 1572.
- Navigation and Vessel Inspection Circular 03-07, published on July 2, 2007. (NB This is a “guidance” document and not legally binding. Still it is put out by the enforcing agency, so it is very important to know.)
- Other important statutes and regulations including the federal SAFETY Act and regulations on SSI (49 CFR 1520).

Take Home Pointers

3. Facility Security Assessment (FSA) and Facility Security Plan (FSP)

- The FSP is the "**law of your port**" and has a critical role in establishing legal duties and risk at your port. It is the Port's plan for carrying out the port's responsibilities for access control and security on its facilities.

- Who must have a Coast Guard approved FSA and FSP

  - **Owner**
  - **Operator**

- As a legal or risk consultant, you may be considered a person with a "need to know" under the Sensitive Security Information rule (49 CFR 1520) what is in your port's Facility Security Assessment (FSA) and Facility Security Plan (FSP). If so, review the plan with your port's security managers and Facility Security Officers (FSOs).

  - **Is it consistent with your Port's Operations Plan?**
  - **Does it go beyond baseline federal security requirements?**

- FSPs are good for five years and then must be reviewed; for most Ports, this is the year for renewal, and so it's a good time for your input.

Take Home Pointers

Here is what the regulations require to be in a FSP – the concept is the idea of "layered security":

33 CFR § 105.405 Format and content of the Facility Security Plan (FSP).

(a) A facility owner or operator must ensure that the FSP consists of the individual sections listed in this paragraph (a). If the FSP does not follow the order as it appears in the list, the facility owner or operator must ensure that the FSP contains an index identifying the location of each of the following sections:

(1) Security administration and organization of the facility;

(2) Personnel training;

(3) Drills and exercises;

(4) Records and documentation;

(5) Response to change in MARSEC Level;

(6) Procedures for interfacing with vessels;

(7) Declaration of Security (DoS);

(8) Communications;

(9) Security systems and equipment maintenance;

(10) Security measures for access control, including designated public access areas;

(11) Security measures for restricted areas;

(12) Security measures for handling cargo;

(13) Security measures for delivery of vessel stores and bunkers;

(14) Security measures for monitoring;

(15) Security incident procedures;

(16) Audits and security plan amendments;

(17) Facility Security Assessment (FSA) report; and

(18) Facility Vulnerability and Security Measures Summary (Form CG–6025) in appendix A to part 105–Facility Vulnerability and Security Measures Summary (CG–6025).

(b) The FSP must describe in detail how the requirements of subpart B of this part will be met. FSPs that have been approved by the Coast Guard prior to March 26, 2007, do not need to be amended to describe their TWIC procedures until the next regularly scheduled resubmission of the FSP.

(c) The Facility Vulnerability and Security Measures Summary (Form CG–6025) must be completed using information in the FSA concerning identified vulnerabilities and information in the FSP concerning security measures in mitigation of these vulnerabilities.

Take Home Pointers

4. Insurance & Risk Resources

- If there is a security incident, do you have a Policy of Terrorism Insurance? What does it cover?
- Do you have SAFETY Act benefits?
- How does FEMA fit into the picture and what will you need to get available federal resources and funds? This is an area where the Risk Manager, Attorney, Security Manager and, ultimately, Senior Management, must all be on the same page.

Take Home Pointers

5. What Security Measures Are in Your Contracts and Leases?

- Do you have provisions requiring tenants, vendors, and other port users to comply with all port regulations on access control and security and with all federal, state and local security laws and regulations, including TWIC?

- Does the provision include an indemnity in case your port is fined for a security breach that was caused by one of these port users?

Take Home Pointers

6. Sensitive Security Information - SSI

- 49 CFR 1520 – SSI includes your FSA and FSP and a host of other security information
- You must be a person who has a “need to know” in order to have access to SSI.
- Requirements for Marking SSI Documents with a Non-Disclosure Statement; Keeping SSI Documents under “Lock & Key”
- Procedures for Protecting SSI in RFP and Other Procurement Situations with Potential Vendors and Consultants (e.g. Design Specs in Security Infrastructure Projects) – Use of Confidentiality Agreements

Take Home Pointers

7. Port Security Grant Program (PSGP)

- The federal Port Security Grant Program (PSGP) is now up to Round 9 (moneys to be appropriated in Fiscal Year '09). The federal Port Security Grant Program has changed for most ports. It is now handled largely at the regional level with a local Grant Committee appointed by the Captain of the Port and a Fiduciary Agent that handles funds disbursed by FEMA and is responsible to see that individual facilities that receive grants are in compliance with grant terms. Grant applications by individual facilities must be consistent with the updated port-wide security assessment and plan. Currently, for public port authorities, there is a 25% matching requirement; there are also restrictions on using grant funds for operations and maintenance expenses. Current favored projects in many port sectors include:
  - **Response side projects, including training, drills and exercises**
  - **TWIC infrastructure projects**
  - **Business continuity**

Note that your Grant Applications May Well Contain SSI – you should mark it as such per the requirements in 49 CFR 1520.

Take Home Pointers

Also, a One-Time Stimulus Grant for This Year:

- **DHS Stimulus Web Resource:** http://www.dhs.gov/xopnbiz/gc_1235067544334.shtm

- **FEMA Port Security Grants - $150 million**
- Cost-share is waived
- Priority for construction projects and those that create jobs. Applicants may need to outline jobs created
- AAPA working with DHS on the criteria for projects
- FEMA expects to announce the criteria and application process on or around May 21, 2009

- NB This grant is subject to further announcement – NEED TO LOOK AT CURRENT LAW AND REGS!

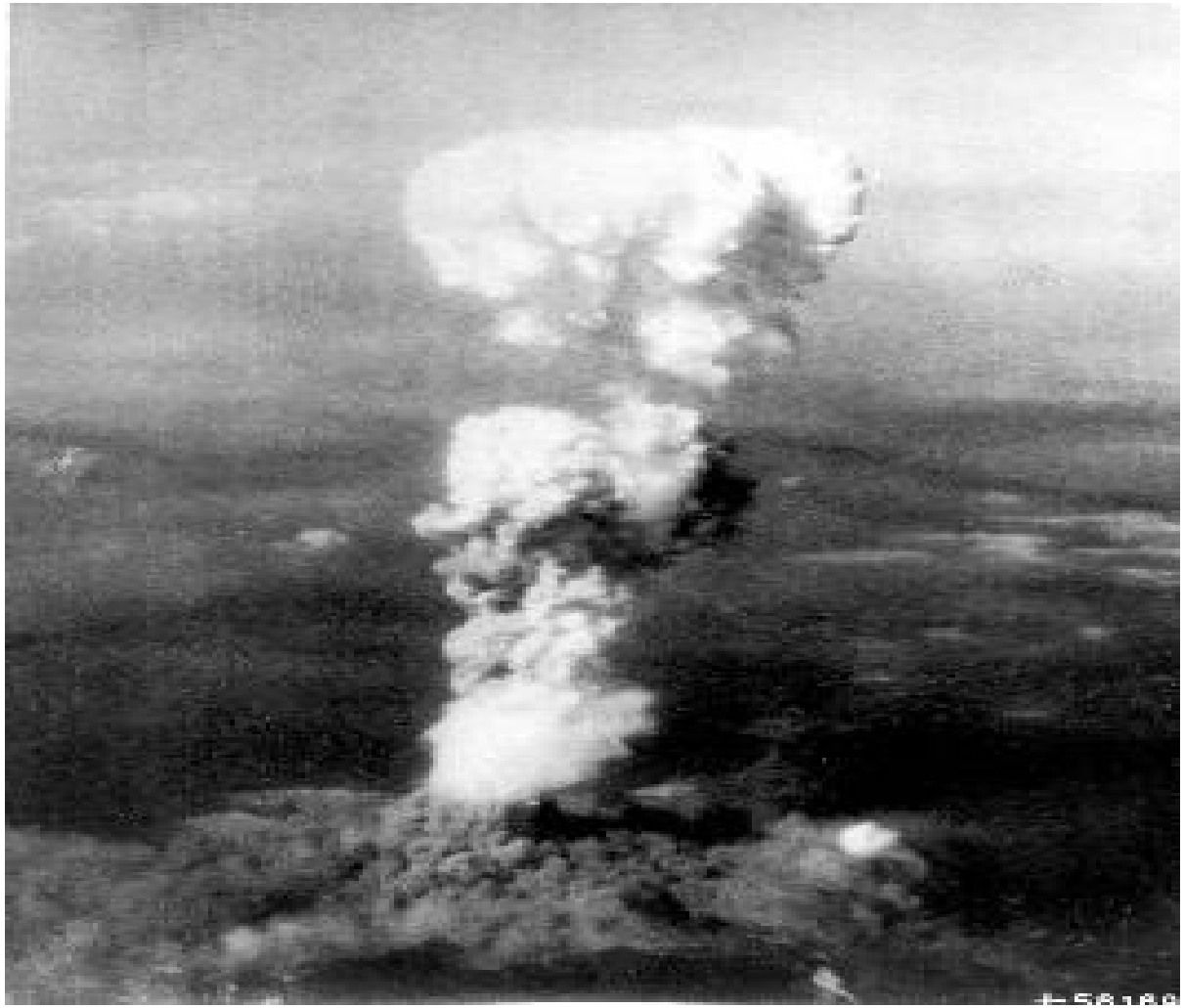
Take Home Pointers

8. Your Port is Unique – What are the Real Threats?

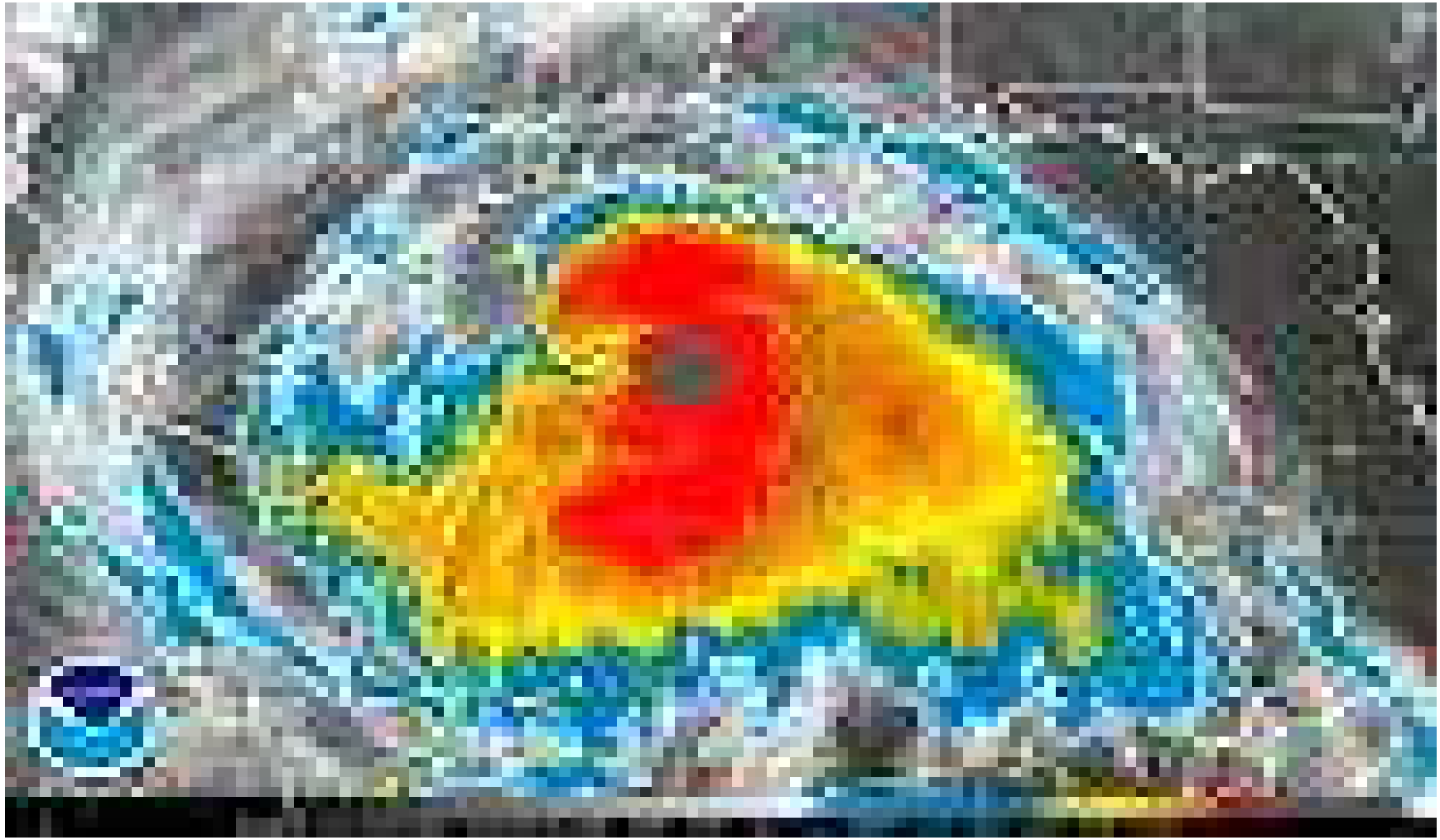
- Concern for a WMD in a container remains due to potential catastrophic consequences
- Now, eight years after 9/11, other threats being considered
  - Catastrophic Weather Events – Katrina, Ike
  - Man-made
    - Cruise Ship Protection
    - Small Boats and Aircraft Dangers
    - Underwater Threats
    - Chemical Plant Explosions; Pipeline Dangers
    - Drugs: The Growing Threat from the South

What Are the Threats?

What Are the Threats?



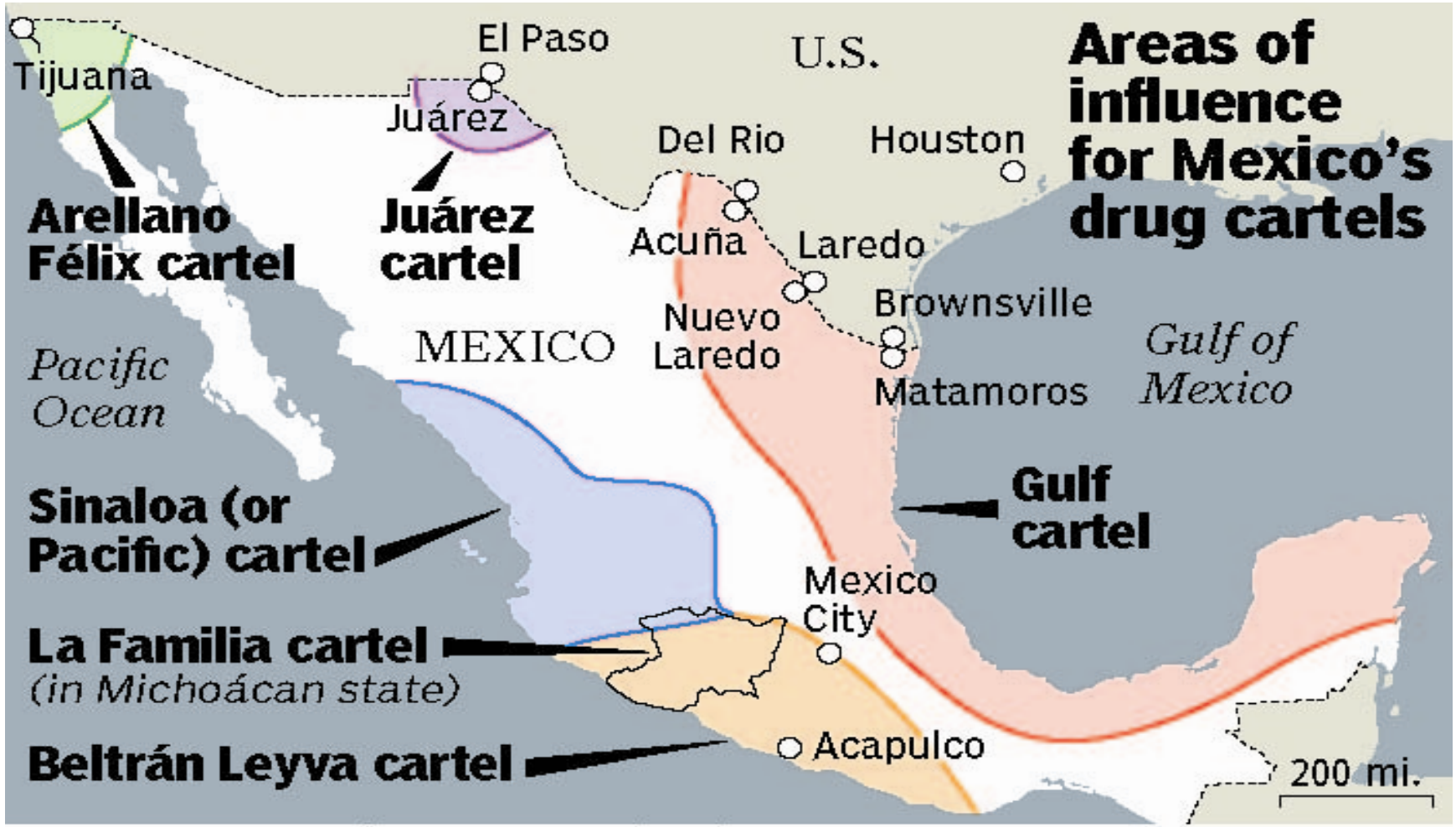
What Are the Threats?



What Are the Threats?

What Are the Threats?

What Are the Threats?



Take Home Pointers

9. Learn More and Stay Abreast of Developments in Maritime Security

- MARSEC Levels
- Emergency Response Plans
  - AAPA Comprehensive "Template" Available
- Equivalency Security Measures 33 CFR § 101.130
- ISO's Security Management System (SMS)
  - Organized Compliance
- Regional Partnerships; Sharing Agreements; Houston Ship Channel Security District (HSCSD)
- Other Laws and Initiatives to Secure Global Commerce, RPMs, CT-PAT, CSI, new "10+2"security filing rules; 100% Cargo Screening – Pros and Cons; CFATS, SAFETY Act, new Rail HazMat Regulations
- Read publications and know the helpful websites – egs., AAPA website; Journal of Commerce; USCG's Homeport
- Don't let the ACRONYMS get to you!

Security Acronyms

- **AMSC** — **Area Maritime Security Committee**
- **CBP** — **Customs and Border Protection**
- **CFATS** — **Chemical Facility Anti Terrorism Standards**
- **33 CFR** — **33 Code of Federal Regulations**
- **CSI** — **Container Security Initiative**
- **C-TPAT** — **Customs-Trade Partnership Against Terrorism**
- **CVI** — **Chemical Vulnerability Information**

Security Acronyms

- **DHS** — **Department of Homeland Security**
- **DoS** — **Declaration of Security**
- **FEMA** — **Federal Emergency Management Agency**
- **FSA** — **Facility Security Assessment**
- **FSO** — **Facility Security Officer**
- **FSP** — **Facility Security Plan**
- **MARSEC** — **Maritime Security Level**
- **MTS** — **Maritime Security Transportation Act of 2002**
- **NIMS** — **National Incident Management System**

Security Acronyms

- **NIPS** — **Network Based Intrusion Prevention System**
- **NMSAC** — **National Maritime Security Advisory Committee**
- **PAC** — **USCG's Policy Advisory Council**
- **PSGP** — **Port Security Grant Program**
- **RPM** — **Radiation Portal Monitors**

Security Acronyms

- **SAFE PORT ACT of 2006** — **Security and Accountability for Every Port**
- **SAFETY ACT** — **Support Anti Terrorism by Fostering Effective Technologies Act of 2002**
- **SSI** — **Sensitive Security Information**
- **TWIC** — **Transportation Workers Identification Credential**
- **USCG** — **United States Coast Guard**

Supply Chain Security Glossary

- **Supply Chain Security Glossary**
- **24-hour Rule** — 24-Hour Electronic Transmission of Advance Cargo Manifests — Twenty-four hours before any container is loaded onto a vessel bound for the United States, **CBP** (see below) receives advanced electronic transmission of cargo manifests. The information is analyzed by CBP's Automated Targeting System (see **ATS** below) to compare against law enforcement data, the latest threat intelligence and the shippers' history in order to identify high-risk cargo shipments that require further review, inspection or denial of loading.
- **AMS — Automated Manifest System**. A multi-modular cargo inventory control and release notification system through which carriers submit their electronic cargo declaration 24 hours before loading (see **24-hour Rule** above).
- **ATS — Automated Targeting System**. A system (computer model) put in place by CBP to detect suspicious shipments, incorporating terrorism related targeting tools by inspecting cargo manifests and combining intelligence on suspicious trading patterns and warnings from other government agencies.
- **Bill of Lading** — Official legal document representing ownership of cargo, a negotiable document to receive cargo, and the contract for cargo between the shipper and the carrier.
- **Carrier (or Freight Carrier)** — Companies that haul freight, also called "for-hire" carriers. Methods of transportation include trucking, railroads, airlines, and sea-borne shipping.
- **CBP — U.S. Customs and Border Protection (CBP)**. Formed during the creation of the Department of Homeland Security in 2003, CBP consists primarily of the customs inspection function formerly performed by the U.S. Customs Service as part of the Department of Treasury, the immigration inspection function formerly performed by the Immigration and Naturalization Service (INS), and the Border Patrol, formerly part of the Department of Justice.
- **Consignor** — see **Shipper** below.
- **CSD — Container Security Device**. An electronic device or system used to secure a container and detect tampering of the container doors.
- **CSI — Container Security Initiative.** A customs-to-customs partnership, CSI represents a security regime to ensure all containers that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the United States. Through CSI, CBP officers work with host customs administrations to establish security criteria for identifying high-risk containers. CSI is currently operational at 44 of the largest foreign ports.
- **C-TPAT — Customs-Trade Partnership Against Terrorism**. A voluntary, joint government-business initiative designed to standardize and ensure the integrity of participating members' security practices and enable cargo to move more efficiently. C-TPAT currently has 5,777 certified members, of which 1,545 have been fully validated and 2,262 are in the process of being validated.

Supply Chain Security Glossary

- **Entry Data** — Cargo data filed at the port of entry to CBP that is used to determine when cargo will be cleared to leave a port. Entry data includes the manufacturer's identification number, the importer's identification number, country of origin of the goods, and a more precise description of merchandise. Appropriate elements of entry data have been deemed to be better than manifest data for risk-targeting.
- **Examination** — As defined by CBP, an examination is either (1) a physical inspection of a container or other conveyance; or, (2) the imaging of a container or other conveyance using large-scale Non-Intrusive Inspection technology.
- **GreenLane** — A concept that would give C-TPAT members that demonstrate the highest standard of secure practices additional benefits for exceeding the minimum requirements of the program. GreenLane benefits would include expedited movement of cargo, especially during an incident of national significance.
- **IMO — International Maritime Organization**. The United Nations' specialized agency responsible for improving maritime safety. Provides mechanism for cooperation among governments regarding regulations and practices relating to technical matters affecting shipping engaged in international trade; encourages and facilitates general adoption of the highest standards regarding maritime safety, efficiency of navigation and prevention of pollution from ships.
- **Importer** — see ***shipper*** below.
- who also provide landside operations.

Supply Chain Glossary

- **Inspecting** — Signifies manual inspection of containers. The government inspects 5.5% - 6% of all inbound containers (those that raise a red flag in the government screening process) using either X-ray or gamma ray technology or through physical inspection of the container. This is the "5%" inspection rate often cited in debate. *syn*. — see **Examination**. (Note: CBP's definition of **Screening** can also mean "Inspecting" as defined here OR the screening of information; see definition of **Screening** below.);
- **ICIS — Integrated Container Inspection System**. A container scanning pilot program in Hong Kong operated by private industry. ICIS blends gamma ray imaging, radiation monitoring and optical scanning equipment. The pilot project is in place at two terminals in Hong Kong.
- **ISO — International Organization for Standardization.** A worldwide federation of national standards bodies from some 130 countries, ISO is a non-governmental organization established in 1947 to promote the development of standardization facilitating international trade. ISO's work results in international agreements that are published as International Standards. (see **Seals**)
- **ISPS — International Ship and Port Facility Security Code** adopted by the IMO (see above) and based on the U.S. MTSA (see below), came into force on July 1, 2004. It is a comprehensive, mandatory security regime for international shipping and port facility operations agreed to by the members of the IMO. Ships must be certified by their flag states to ensure that mandated security measures have been implemented; port facilities must undergo security vulnerability assessments that form the basis of security plans approved by their government authorities.
- **Joint Operation Centers for Maritime Security** — Centers to be established to ensure a coordinated response and the rapid resumption of the flow of commerce in the event of a maritime security incident and co-located with Coast Guard sector command centers, approximately 15-20 nationwide. Primary responsibilities to include: facilitating cooperation between private sector and government security agencies (at local, state, and federal levels), sharing of information and intelligence related to cargo security, and lead local after-incident response for trade resumption.
- **Manifest** — Document that lists in detail all the bills of lading (see above) issued by a vessel or its agent or master, i.e., a detailed summary of the total cargo of a vessel. Used principally for customs purposes. Also known as "summary of bills of lading."

Supply Chain Security Glossary

- **MTSA — Maritime Transportation Security Act**. Law passed in 2002 to create a comprehensive national system of transportation security enhancements. The MTSA designated the U.S. Coast Guard as the lead federal agency for maritime homeland security and requires federal agencies, ports, and vessel owners to take numerous steps to upgrade security. The MTSA requires the Coast Guard to develop national and regional area maritime transportation security plans and requires seaports, waterfront terminals, and vessels to submit security and incident response plans to the Coast Guard for approval. The MTSA also requires the Coast Guard to conduct antiterrorism assessments of certain foreign ports.
- **OBL — Ocean Bill of Lading (Ocean B/L)**. Document indicating that the exporter will consign a shipment to an international carrier for transportation to a specified foreign market. Unlike an inland B/L, the ocean B/L also serves as a collection document. [Note: for **Original** Bill of Lading, see definition for ***Bill of Lading*** above.]
- **NII — Non-Intrusive Inspection technology**. Originally developed to address the threat of smugglers using increasingly sophisticated techniques to conceal narcotics deep in commercial cargo and conveyances, NII systems, in many cases, give Customs inspectors the capability to perform thorough examinations of cargo without having to resort to the costly, time consuming process of unloading cargo for manual searches, or intrusive examinations of conveyances by methods such as drilling and dismantling.
- **NVOOC — Non Vessel Owning Ocean Carrier**. (a) A cargo consolidator of small shipments in ocean trade, generally soliciting business and arranging for or performing containerization functions at the port. (b) A carrier issuing Bs/L for carriage of goods on vessel which he neither owns nor operates.
- **Port authorities** — Local government entities whose role is akin to landlords that lease lots for a wide variety of activities, including cargo loading and unloading. Port authorities are not responsible for providing shore-side operations, which is the responsibility of terminal operators (see below) or steamship operators

Supply Chain Glossary

- **RFID — Radio Frequency Identification**. Technology used for tracking. RFID tags can be used to track container movements based on a radio frequency signal. Radio frequency transceivers are now in common use. The latest radiation detection portals and container scanning equipment are being combined into a single unit and capture images of trucks moving at speeds up to ten mph. Large ports would need several to ensure that the screening process would not slow the flow of trucks.
- **Seal (container seal)** — A device fastened to the doors of a container used to secure its contents and insure the integrity of a shipment. Standardization of seal types, including definition of "high-security seal", is established by ISO (see above).
- **“Smart” Seal (e-Seal)** — Next generation technology — a container seal that is intended to be "more secure" than a mechanical seal and can include information such as manifest information. Requires a centralized database to receive and process the information. Variations on smart seal concepts include seals designed to track the time and location of a container during transit, including by truck, rail, or vessel.
- **Screening (1)** — Customs and Border Patrol (CBP) defines screening as a passive means of scanning a conveyance, baggage or cargo. CBP screens conveyances, baggage, and cargoes with radiation portal monitors and other radiation detection equipment for the presence of radiological emissions — i.e., nuclear screening.
- **Screening (2)** — CBP also use the term "screen" to describe the targeting and risk management process. CBP **screens** information on 100% of import containers through its ATS (see above) 24 hours before they are loaded onto US-bound vessels. Each and every container identified as high risk is subsequently inspected either in the foreign port of loading or upon arrival in the U.S. by CBP. (see **Inspecting**)
- **Shipper** (or consignor) — The person or entity for whom the owners of a ship agree to carry goods to a specified destination at a specified price.

Supply Chain Security Glossary

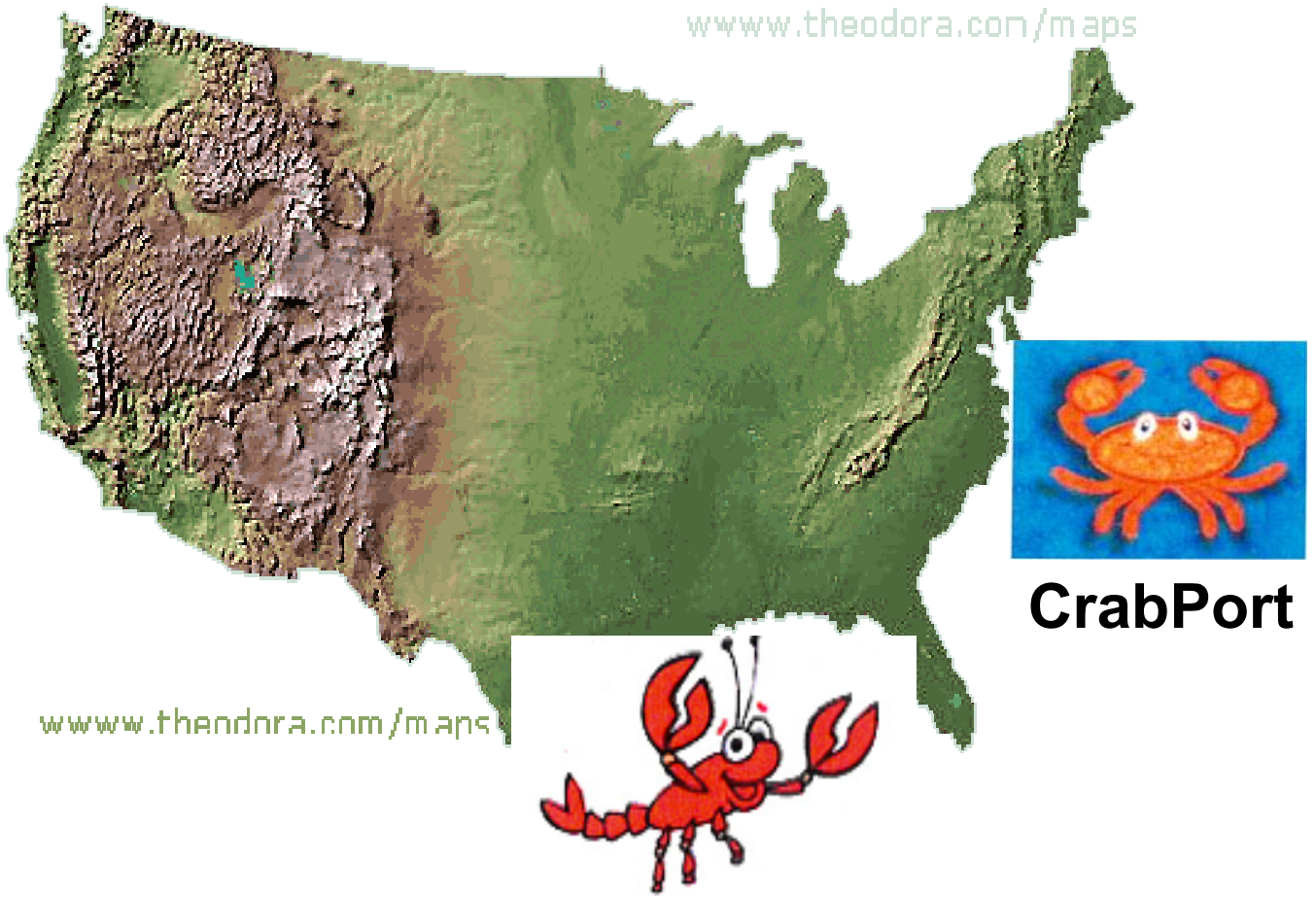
- **Stevedore** — Company that provides equipment and hires workers to transfer cargo between ships and docks. Stevedore companies may also serve as terminal operators. The laborers hired by the stevedoring firms are called stevedores or longshoremen.
- **Terminal operator** — The company that operates cargo handling activities on a wharf. A terminal operator oversees unloading cargo from ship to dock, checking the quantity of cargoes against the ship's manifest (list of goods), transferring of the cargo into the shed, checking documents authorizing a trucker to pick up cargo, overseeing the loading/unloading of railroad cars, etc.
- **TSA – Transportation Security Administration**. TSA was created in response to the attacks of September 11th and signed into law in November 2001. TSA was originally in the Department of Transportation but was moved to the Department of Homeland Security in March 2003. TSA's mission is to protect the nation's transportation systems by ensuring the freedom of movement for people and commerce.
- **TWIC — Transportation Workers Identification Credential**. TSA's TWIC program is meant to improve security by establishing a tamper resistant common credential to be used by personnel who require access to secure and sensitive areas of the nation's transportation system. The TWIC uses biometric information about the cardholder to positively authenticate identity of holders. Mandated by Congress.
- **U.S. Coast Guard** — The Coast Guard is the lead federal agency for maritime security. The Coast Guard Captain of the Port is the lead federal security officer at U.S. ports.
- **VACIS** — **Vehicle and Cargo Inspection System technology**. VACIS is an advanced technology that uses a gamma ray imaging system to provide a non-invasive image of cargo contents. CBP has placed VACIS technology at major cargo terminal facilities throughout the nation to inspect containers for dangerous substances and devices.

Take Home Pointers

10. You Can Make a Difference!

- Finally, realize that you have something to contribute to port security. Our total port security system nationwide is only as strong as the weakest links. So even if you don't believe that your port is a potential terrorist target, remember that you don't know how the terrorists think, that there may be other threats to your unique port environment, and if your port is secure and you are part of the port security team, you have made a real contribution to national security.

Fact Patterns Involving Two U.S. Ports



CrabPort

CrawPort

Fact Pattern No. 1 – CrabPort

THE FIRST TRANSPORTATION SECURITY INCIDENT (TSI):

CrabPort

On July 4, 2009, at the Port of Crabcake Bay (a/k/a CrabPort) located in a state of the U.S. on the East Coast, a fire truck arrived at the Port's main gate in response to a fires set in a warehouse located on the waterfront. Although the Port's security guards, trained by their company and the Port's Security Department in matters concerning the Transportation Workers Identification Credential (TWIC), let the fire truck and its occupants proceed into the Port's secured and restricted areas and proceed to the scene of the fire at the waterfront warehouse. No one on the fire truck had a TWIC and the CrabPort security guards did not ask if they did.

Fact Pattern No. 1 – CrabPort

- No breach is involved. Under section 3.1c of NVIC 03-07, emergency responders (i.e., emergency responders employed by a government agency and medical personnel when responding to an emergency situation) are exempt from the requirement of needing a TWIC for unescorted access to a port's secured and restricted areas.
- All security personnel must be trained per 33 CFR 105.210.
- This exemption could be a loophole for a terrorist plot – as it is in this hypothetical. The question is: how to balance the need for expedited emergency response with the need for access control at our ports.
- TWIC rules are critical for port facility owners and operators. They are the ones who get the Notice of Violation, fines and other penalties from the Coast Guard – not the trucker or other individual who fails to comply with TWIC regulations.

Fact Pattern No. 1 – CrabPort

Upon arrival at the warehouse, the occupants of the fire truck quickly and easily extinguished the fire, but also, unseen by any others, loaded some cargo stored in a corner of the warehouse into a bay of the fire truck.

Since the cargo was not stored in a container, the fire truck was able to bypass the Port's Radiation Portal Monitors (RPMs), operated by US Customs & Border Patrol (CBP), and exit from the Port without detection.

Fact Pattern No. 1 – CrabPort

- CBP's Radiation and Portal Monitor program only addresses the requirement of 100% container screening at US ports. Thus, another potential loophole in security regulations. The perception has always been that the greatest need is to protect against a weapon of mass destruction smuggled in a container. Currently, improvements to the RPM program technology are underway.

- There is a growing perception that our seaports are not, in fact, the likely entry points for smuggling of WMDs, and that the borders are the more likely smuggling point. Port operators are in a competitive environment and thus tend towards skepticism about increasing security regulations that slow down the movement of cargo. The only resolution would seem to be a technology that would allow radiation screening of all cargoes without slowing down commerce.

Fact Pattern No. 1 – CrabPort

- Approximately two hours later, the City of CrabPort's downtown was devastated by a "dirty" radioactive bomb. Thousands of people were killed and severely injured by the blast which continued to pollute the air in a deadly manner throughout the downtown and inner city.
- Panic ensued as people attempted to evacuate. One school attempted to "shelter in place," but the technology which was supposed to seal the building off from outside radioactivity was faulty, even though it had been U.S. SAFETY Act certified.

Fact Pattern No. 1 – CrabPort

- The Port Security Grant Program is currently focusing on response-side projects. Shelter-in-place buildings that can protect against radiation from smaller radioactive weapons may be part of a region's overall emergency response plan. In large urban areas like Houston, it would take days, not hours, to evacuate the population, so alternative responses involving sheltering in place may be required.

- Brian Finch will discuss SAFETY Act implications.

Fact Pattern No. 1 – CrabPort

The event, referred to as a Transportation Security Incident (TSI) in federal security regulations, was a total catastrophe. Lawsuits were quickly filed alleging multiple theories of recovery. Among the many defendants were CrabPort, the security guard company, the CBP, and the respective manufacturers/developers of the hand-held nuclear detector and the Port's Master Security Plan & Emergency Response Program – MSP&ERP (each of which was purchased with a grant from the federal Port Security Grant Program, although since the Program did not include Operation and Maintenance Expenses, the Port, under severe pressure because of the current economic crisis, had neglected upkeep of the detector and proper training under the MSP&ERP). Among their defenses, they each pleaded immunity under the federal SAFETY Act. They also attempted to prevent discovery of evidence, alleging that it constituted "Sensitive Security Information" under 49 CFR 1520 and the federal statues under which this regulation was promulgated.

Fact Pattern No. 1 – CrabPort

- **Under federal regulations in 33 CFR, a port must have a Facility Security Plan (FSP) approved by Coast Guard. A port is required to have a response plan and be able to respond to security incidents and changes in MARSEC levels. 33 CFR Section 105.405; 105; 280.**
- **Lawyers and Risk Managers are advised to consult with your port's Security Managers and review this Plan.**
- **The AAPA has a "template" Emergency Response Procedures developed under the leadership of Phyllis Saathoff, Managing Director of the Port of Freeport. You might use it to see what might be included in the Emergency Response section of your port's Facility Security Plan.**
- **Again, however, remember that the FSP, once approved by Coast Guard, in effect becomes the law of your port. While you must provide for the minimum requirements set forth in 33 CFR Section 105.405, by the same token, you want to be careful about overburdening your port with expensive, resource-intensive security requirements that go above and beyond what the regulations and Coast Guard require.**
- **As to the lawsuits and legal consequences of this TSI, Brian will give us some insights in a just a few minutes.**
- **As to the defense pertaining to Sensitive Security Information, Steve Roberts will give us some insights in his presentation.**

Fact Pattern No. 1 – CrabPort

In response to discovery requests concerning insurance, the Port acknowledged that it carried a policy of terrorism insurance. CrabPort's Risk Manager and General Counsel met to analyze the amount, coverage, and collectability of this insurance in the face of the TSI.

The Plaintiffs, not content to use solely the court rules for discovery, made numerous requests under the federal Freedom of Information Act (FOIA) as well as its state version.

Public demand ensued to stay the litigation, and legislation was introduced to enjoin all litigation concerning the TSI.

Fact Pattern No. 1 – CrabPort

- Some ports have a Policy of Terrorism. The issues for Risk Managers, Attorneys and Security Managers include:
- What are the coverages under such a policy?
- Do the coverages include matters above and beyond more conventional insurance policies and umbrella policies?
- How does the SAFETY Act interact and effect these policies?
- What is available from FEMA in the event of a TSI? The Port of Houston Authority suffered certain damages to its security infrastructure as a result of Hurricane Ike, and FEMA has approved the claim presented by our Risk Manager.

Fact Pattern No. 2 – CrawPort

CrawPort

A. The Truck. On September 11, 2009, at the Port of Crawfish Bayou (a/k/a CrawPort), located in a state of the United States on its Gulf Coast, in an area with a heavy concentration of chemical and petrochemical refineries, a truck driver arrived in a truck bearing foreign plates. He presented a TWIC to Crawport's security guards. Unknown to the security guards, the driver was a convicted felon, having been tried and found guilty on separate occasions of arson, possession of explosive devices, improper transportation of a hazardous material, and sales of illegal drugs. Along with the driver, there was also a passenger in the truck who did not possess a TWIC.

The security guards, trained in TWIC procedures by the CrawPort FSO, did a "flash pass" check of the driver's TWIC and the passenger's driver's license and let them onto CrawPort Road which led into CrawPort's restricted area where chemical tank farms and a maze of chemical pipelines were located next to CrawPort Road and the United Specific Rail Road (USRR) tracks.

Fact Pattern No. 2 – CrawPort

- The truck driver may have legitimately obtained a TWIC despite his convictions for felonious crimes. Under 49 CFR 1572.103 and 49 CFR 1515.7, a person may be convicted of these crimes and request a waiver on the argument that notwithstanding these crimes, he is not a security threat at the port's facilities' restricted and secured areas.

- Presently, all that is required is a "flash pass" check of a TWIC to determine that the photo lines up with the person presenting the card, the card is not damaged, and the card has not expired. See NVIC 03-07 ; 33 CFR 105.255. No reader requirements are presently in place, and so the TWIC's biometric information, stored in the card's computer chip, is of no use except perhaps when Coast Guard conducts random checks.

- The truck driver may (but is not entitled to) act as an escort of the passenger of the truck. This is at the discretion of the FSO of the port's facility. At the Port of Houston, no one may act as a TWIC escort without possessing a valid TWIC and having taken the Port's TWIC training class and having signed a document indemnifying the Port against any fines on account of the escort's breach of escort rules and procedures

Fact Pattern No. 2 – CrawPort

B. CrawPort's Escort Monitoring and Responsive Software Systems. The truck driver and occupant in his vehicle were monitored by sophisticated security cameras linked to CrawPort's Emergency Operations Center computers which possessed "Intelligent Video" software as well as chemical release tracking software ("ChemRelease"). ChemRelease was designed, in the event of a chemical release into the atmosphere, to identify chemical types, dangers, wind speed and direction in order to trace the path of toxic airborne chemicals, residential areas that would be affected, projected times and routes for evacuation and locations of buildings with sheltering-in-place systems, and the contact information for personnel with emergency response capabilities for the released chemical. Both of these systems, Intelligent Video and ChemRelease, were SAFETY Act certified.

Fact Pattern No. 2 – CrawPort

When the truck driver proceeded into CrawPort's restricted areas, the escort rules required a 5 to 1 live side by side ratio, rather than monitoring by security cameras. If the truck driver, who possessed a TWIC, had taken CrawPort's escort training, then, under CrawPort's requirements, the truck driver may have been able to act as an escort. Otherwise, the occupant of the truck was not correctly escorted and the camera monitoring, although perhaps providing security, was not enough to avoid a breach of the TWIC regulations.

Brian Finch will tell us about the SAFETY Act and the benefits of certification for the vendor of technology and the buyer (the port).

Fact Pattern No. 2 – CrawPort

C. <u>The Train.</u> As the truck driver made his way into the restricted area, a USRR train arrived at CrawPort.

At the rail gates, the security guard checked the conductor's TWIC up at the front of the train (but not the non-TWIC holding rail worker at the back of the train) and let the train proceed into CrawPort where it was scheduled to off-load load chlorine, ammonia and certain other explosive chemicals classified by federal regulations as hazardous materials.

Fact Pattern No. 2 – CrawPort

- A lot of attention has been given to TWIC requirements as they apply to the rail sector. One of the major railroads, in particular, has, for a long stretch of time, resisted acknowledgment of the TWIC rules and their application to rail workers. The TWIC Policy Advisory Council (PAC) has issued a publication pertaining to TWIC and rail workers. See TWIC Requirements and Rail Access into Secure Areas, PAC 05-08. Under this Policy, "a front-of-train TWIC holder, back-of-train non-TWIC holder will generally not qualify as an acceptable arrangement for a locomotive moving multiple railroad cars…."

Fact Pattern No. 2 – CrawPort

D. <u>The Mariner Bus</u>. Also at this time, some thirty (30) mariners, none of which were U.S. citizens, and none of which possessed TWICs, debarked from a vessel working at CrawPort's docks and got into a bus (the "Mariner Bus") driven by a TWIC holder. The Mariner Bus headed towards CrawPort's Main Gate.

Fact Pattern No. 2 – CrawPort

Fact Pattern No. 2 – CrawPort

Another exception to the TWIC Basic Rule and the 1 to 5 escorting ration is when you transport a group in or out of restricted or secure areas, such as mariners working on the vessels. In this situation, as long as someone in the transporting vehicle is a TWIC holder and qualified TWIC escort. So here, the bus driver, if having satisfied any applicable training or other requirements set by CrawPort, can legally transport more than 5 mariners at one time either off the vessel and out of the restricted or secure areas of CrawPort or back onto the vessel later on. See NVIC 03-07, Section 3.3 c (3): "Escorting ratios do not apply when non-TWIC holders are transported in an enclosed vehicle. In this case, one TWIC holder who is driving or riding in the vehicle can escort any number of passengers as long as they are only allowed to depart the vehicle in a location where other TWIC holders will be able to escort them or where they will not need to be escorted…."

COMPANY NAME

SHORE ACCESS ESCORT FOR PERSON(S) NOT HOLDING A TRANPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC)

Date: _____ Time: _____

Current MARSEC Level: _____

I acknowledge the following responsibilities as an escort into the Secure Area:

1. I am responsible for assuring that none of the persons listed on this card enter a Secure Area without my personal escort, and must maintain close contact with all individuals that I will be escorting.
2. I may only escort 10 individuals in a Secure Area, and only 5 individuals in a Restricted Area, unless they are within the confines of my vehicle.
3. I am only authorized to escort the individuals listed to and from the vessel through the facility. I am not authorized to escort individuals involved in work activities within the facility.
4. I am responsible for monitoring the individuals that I am escorting for any unusual activity that may pose a threat to the security of the facility.
5. If the person(s) I am escorting engage in activities outside of those for which the escort is provided, I will notify xxx at xxx.
6. I understand that violation of the escort policy may result in disciplinary action, loss of access privileges, and may involve a violation of Federal regulations.
7. By assuming this responsibility I am acknowledging that I have a valid TWIC in my possession.
8. Baggage, stores and other materials that are to be carried through the facility will be screened by facility security personnel prior to entering the facility, and by xxx when coming from

_____

Signature

_____

Escort Badge/ID Number

Escort between: _____

and: _____

Individuals being Escorted:

_____

Name (1)

_____

Name (2)

_____

Name (3)

_____

Name (4)

_____

Name (5)

_____

Name (6)

_____

Name (7)

_____

Name (8)

_____

Name (9)

_____

Name (10)

_____

Name (11)

_____

Name (12)

_____

Name (13)

_____

Name (14)

_____

Name (15)

Fact Pattern No. 2 – CrawPort

E. <u>The Construction Worker Bus</u>. At the same time, 25 persons, none of whom possessed a TWIC but identifying themselves as construction workers on a project in CrawPort's restricted area, arrived at CrawPort's Main Gate in another bus (the "Construction Worker Bus") driven by a non-TWIC holder and, with the consent of the security guards, they were escorted by the Mariner Bus into CrawPort's restricted area. The two buses drove towards the chemical tank farms.

Fact Pattern No. 2 – CrawPort

- The TWIC Basic Rule is easy (you must have a TWIC for unescorted access into a port's restricted and secure areas). The problem is that enforcement of this rule without exceptions would render a port and its many different users and stakeholders unable to carry out its many activities and operations. So, for example, we had the exception for emergency response workers in the first fact pattern at CrabPort.

- At Section 3.3 c (6) of NVIC 03-07, there is a segment on TWIC and construction workers. We have met with our local Coast Guard representatives in Houston, and they have confirmed that the usual 1 to 5 or 1 to 10 escort ratios do not apply where a construction project takes place in a restricted or secure area as long as certain conditions are met, including placing fencing around the construction site to effectively segregate it from the operational portions of the restricted or secure areas.

Fact Pattern No. 2 – CrawPort

F. <u>The Cyber Attack</u>. At the same time as the truck drive and USRR train arrived at CrawPort, CrawPort's computer system was hit by a Cyber attack that effectively knocked out its security cameras and Intelligent Video system. Thus, the truck, train and buses all proceeded freely into CrawPort's restricted areas without further monitoring or detection.

Fact Pattern No. 2 – CrawPort

Many experts believe that cyber attacks will be the terrorists' "weapon of choice' in the future. We have all read about the possibilities, from crippling of our communication systems, theft from our financial institutions to identify theft.

Current Port Security Grant Program projects include "hardening" of a port's computer software and hardware against attack. This includes redundancy projects and back-up systems.

Fact Pattern No. 2 – CrawPort

G. **The Storm.** The only thing more ominous at CrawPort than the suspicious characters and activities that day was the threatening sky. Shortly after the arrival of the truck, the train and the two buses, CrawPort was suddenly hit by a fierce tropical storm that had unexpectedly picked up hurricane-force winds in the bath-like late-summer Gulf, The storm took an unanticipated trajectory directly through CrawPort. The senior weather analyst at the National Weather Service, being down to the "L's" in the alphabet for naming storms, named it "Like Ike". Like Ike had very strong surge-producing winds, and a relentless rain which quickly flooded the low-lying CrawPort and prevented those arriving on the truck, train and vessel from carrying out any activities.

Like Ike's ferocity quickly uprooted trees, made flying projectiles from ripped warehouse roofs and snapped light poles, tossed the truck on its side, de-tracked the train, chased the buses out of the port, and put an immediate stop to the plans and schemes of all their occupants. In short, Like Ike was the hero of the day.

H. **CrawPort's Storm Response Using its Security Infrastructure**. CrawPort utilized its back-up (redundant) systems to overcome the Cyber attack. With its video data sharing arrangements with the U.S. Coast Guard and the State Highway Transportation Department, it was able to assist in tracking of the storm path and facilitate evacuation of the populace in an orderly fashion.

Meanwhile, the security guards, noticing the truck lurking in the restricted area of the truck farm, stopped, detained and arrested the truck driver when he could not produce his TWIC..

Fact Pattern No. 2 – CrawPort

The United States Coast Guard does not require a port, or its security personnel, to detain and arrest an individual when he/she cannot produce a TWIC while in, or requesting access to, the port's restricted or secured areas.

Rather, the security personnel should deny access (or tell the individual to immediately leave) the restricted or secured area and report the breach to the Coast Guard.

If an individual presents a fraudulent TWIC, the guards may confiscate the fraudulent TWIC and contact law enforcement as well as the Coast Guard and cause the arrest of the individual based on illegal presentation of a fraudulent TWIC.

Fact Pattern No. 2 – CrawPort

On a larger scale, CrawPort executed successfully its Emergency Operations and Continuity of Operations (COOP) plan (which was part of its USCG-approved Facility Security Plan or FSP), using, among other things, its sonar arrays to test the depth of its ship channel for proper depth since Like Ike's storm surge could have adversely affected the depth required for vessels.

CrawPort was re-opened in a matter of several days and the port business for the CrawPort region was saved along with countless jobs in the community.

Fact Pattern No. 2 – CrawPort

When Hurricane Ike hit the Port of Houston, the U.S. Coast Guard Captain of the Port assembled a Port Coordination Team which included representatives from the Port of Houston Authority, the U.S. Army Corps of Engineers, the Houston Pilots, several of the private petrochemical and chemical plants, the West Gulf Maritime Association (which communicates with the stevedore industry), the barge and tugboat industries and various others, in an effort to re-open the Port of Houston as soon as possible. In fact, the Port was re-opened within five days after Hurricane Ike hit the Port. Both the Area Maritime Security Committee and individual facilities such as the Port of Houston Authority, are required, under MTSA and 33 CFR, to have emergency response plans as part of their Security Plans.

A Port's emergency response team should include legal counsel and the risk manager to assist not only in the response (to ensure compliance with the port's FSP and applicable regulations) but also in the post-incident claims by and against the Port, including claims against the Port's insurance companies and FEMA.

Fact Pattern No. 2 – CrawPort

Meanwhile, Like Ike had long gone north and was busy ravaging the docks and vessels at WindPort and CarPort in the Great Lakes region of the United States.

Fact Pattern No. 2 – CrawPort

This is what happened not only with Hurricane Ike but also with the great hurricane of 1900 that ravaged Galveston and caused a loss of 6,000 lives.

The storm paths were quite similar, and in both cases, the weather experts were surprised at how much damage was caused by these hurricanes more than a thousand miles inland.

Fact Pattern No. 2 – CrawPort

I. **Recovery Alternatives**. CrawPort's General Counsel and Risk Manager then met to review CrawPort's insurance policies and to prepare for months of meetings with FEMA in which CrawPort's storm damage claims were asserted. An issue arose as to whether the best recovery for damages was through (1) FEMA's storm disaster recovery program, (2) FEMA's Port Security Grant Program, or (3) the Administration's new Stimulus package for ports.

Fact Pattern No. 2 – CrawPort

Again, it is necessary to have a post-incident team knowledgeable in how to assert and defend against claims associated with the incident. There may be, as with Hurricane Ike, multiple resources for assistance to recover from the incident.

The Wednesday morning presentations at this Conference covered the critical concerns that risk managers and counsel will have, including integration of FEMA claims and insurance policy claims. For example, FEMA disaster assistance is generally only available for damages or losses not covered by insurance – it is supplemental only.