MTSA

Marine Transportation Security Act

A presentation by:

Petty Officer Kevin McDaniel

U.S. Coast Guard

Port of Miami Field Office:

(786) 777-0775

24hr Duty Phone:

(786) 295-8995
MTSA
Introduction
There are 3 types of U.S.C.G. Facility Inspections:

1) MTSA Security Spot Checks

2) Unannounced Semi-annual Inspection

3) Annual (Announced) Safety / Security Exam
33CFR105.225 RECORDKEEPING REQUIREMENTS

(a) Unless otherwise specified in this section, the Facility Security Officer (FSO) must keep records of the activities as set out in paragraph (b) of this section for at least 2 years and make them available to the Coast Guard upon request.

(b) Records required by this section may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized deletion, destruction, or amendment. The following records must be kept:

Training. For training under §105.210, the date of each session, duration of session, a description of the training, and a list of attendees;

Drills and exercises. For each drill or exercise, the date held, description of drill or exercise, list of participants, and any best practices or lessons learned which may improve the Facility Security Plan (FSP): 33CFR105.220

Incidents and breaches of security. For each incident or breach of security, the date and time of occurrence, location within the facility, description of incident or breaches, to whom it was reported, and description of the response; 33CFR105.280 & 33CFR101.305(b)

Security threats. For each security threat, the date and time of occurrence, how the threat was communicated, who received or identified the threat, description of threat, to whom it was reported, and description of the response; 33CFR105.280(a) & 33CFR101.305(a)

Changes in MARSEC Levels. For each change in MARSEC Level, the date and time of notification received, and time of compliance with additional requirements; 33CFR105.230

Maintenance, calibration, and testing of security equipment. For each occurrence of maintenance, calibration, and testing, record the date and time, and the specific security equipment involved, 33CFR105.250

Declaration of Security (DoS) A copy of each single-visit DoS and a copy of each continuing DoS for at least 90 days after the end of its effective period; and 33CFR105.245

Annual audit of the FSP. For each annual audit, a letter certified by the FSO stating the date the audit was completed. 33CFR105.305

Any record required by this part must be protected from unauthorized access or disclosure. 49CFR1520

What should **YOU** be looking for on MTSA regulated facilities?
• **Security Threat** means any suspicious activity that could result in Security Incident, Breach of Security or Transportation Security Incident (TSI).

• **Maritime Security Incident** means an attempt to breach at least one layer of security measures in place.

• **Breach of Security** means an incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated.

• **Transportation Security Incident (TSI)** means a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.
Is your Facility Secure?
Who should be notified in the event of any type of security incident?
National Response Center

1 (800) 424-8802
... So, I see you’ve got access control in order. I guess I can assume you all have your TWIC’s?
A WORD ABOUT
TRANSPORTATION WORKER IDENTIFICATION CREDENTIALS (TWIC)
**TWIC Overview**

- Under the Maritime Transportation Security Act (MTSA) and Security and Accountability for Every (SAFE) Port Act, the Secretary must establish rules to prevent an unauthorized person from getting into a secure area of a vessel or facility that has a security plan.

- The TWIC rules are based on these two laws. The laws require using a standard, biometric ID (also known as a “credential”), for access control to secure areas of vessels and facilities. The ID is called the “Transportation Worker Identification Credential” or “TWIC.”

- To get a TWIC, individuals must pass a Security Threat Assessment (STA). That assessment helps TSA decide if he or she poses a risk to transportation.
What a TWIC Looks Like

• Front and Back views of a TWIC
TWIC is a Smart Card

- 64K of non-volatile memory
- Dual interfaces share memory
  - Contact interface (ISO/IEC 7816)
  - Contactless interface (ISO/IEC 14443)
- Physical security features
  - Tamper resistant
  - Color shifting inks
- Logical security features
  - Two encrypted fingerprint templates
  - Signed data
  - PKI certificates
TWIC VERSES OTHER QUALIFYING CREDENTIALS
TWIC & Law Enforcement Officials & Other Regulatory Agencies

- Law enforcement officials at the State or local level, are not required to obtain or possess a TWIC to gain unescorted access to MTSA regulated facilities.

- State and local law enforcement officials may use this exemption in the course of their official duties.

- A law enforcement official for the purpose of TWIC to be any officer or employee of any agency or authority of the United States, a State, a commonwealth, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:
  - Investigate or conduct an official inquiry into a potential violation of law; or
  -Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law;
  - and is doing so while acting in their official capacity.

- State environmental officials and others with regulatory enforcement responsibilities at the State and local level who meet these criteria are not required to obtain a TWIC to gain unescorted access. However, they may voluntarily obtain a TWIC.

  - State and municipal fire departments and their officials who require access to secure areas of MTSA facilities for regulatory inspections in conjunction with their official duties fall within the definition given above, and as such are not required to obtain a TWIC or be escorted, as they are considered law enforcement officials. However, they may voluntarily obtain a TWIC.
List of Agencies Qualifying for the “Federal Officials” Exemption

- Army Corp of Engineers
- Centers for Disease Control
- Federal Bureau of Investigation
- Federal Emergency Management Agency
- Federal Grain Inspection Service
- Federal Railroad Administration
- National Marine Fisheries
- National Oceanographic & Atmospheric Administration
- National Science Foundation
- National Transportation Safety Board
- Pipeline & Hazardous Materials Administration
- Transportation Security Administration
- US Postal Service
- US Secret Service

- US Coast Guard
- US Customs & Border Protection
- US Department of Agriculture
- US Department of Defense
- US Department of Energy
- US Department of Homeland Security
- US Department of Interior
- US Department of Transportation
- US Drug Enforcement Agency
- US Environmental Protection Agency
- US Immigration & Customs Enforcement
- US Maritime Administration
- US Marshals Service
- US Nuclear Regulatory Commission
A WORD ABOUT
MARITIME SECURITY
(MARSEC) LEVELS

MARSEC LEVEL
1 2 3

SIGNIFICANT RISK
U.S. Coast Guard Maritime Security (MARSEC) Levels

The Coast Guard has a three-tiered system of Maritime Security (MARSEC) levels consistent with the Department of Homeland Security’s Homeland Security Advisory System (HSAS). MARSEC Levels are designed to provide a means to easily communicate pre-planned scalable responses to increased threat levels. The Commandant of the U.S. Coast Guard sets MARSEC levels commensurate with the HSAS. Because of the unique nature of the maritime industry, the HSAS threat conditions and MARSEC levels will align closely, though they will not directly correlate.

MARSEC levels are set to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the U.S.

**MARSEC Level 1** means the level for which minimum appropriate security measures shall be maintained at all times. MARSEC 1 generally applies when HSAS Threat Condition Green, Blue, or Yellow are set.

**MARSEC Level 2** means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident. MARSEC 2 generally corresponds to HSAS Threat Condition Orange.

**MARSEC Level 3** means the level for which further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable, imminent, or has occurred, although it may not be possible to identify the specific target. MARSEC 3 generally corresponds to HSAS Threat Condition Red.

**How do I add the MARSEC Level to my web site?**

To add the current MARSEC Level to your web site, insert the following tag into your HTML source code:

```html
<script type="text/javascript" src="http://www.uscg.mil/safetylevels/levels.js"></script>
```
SECURITY NOTICE

This facility is currently operating at MARSEC LEVEL 1

BOARDING THE VESSEL OR ENTERING THIS FACILITY IS DEEMED VALID CONSENT TO SCREENING OR INSPECTION

FAILURE TO CONSENT OR SUBMIT TO SCREENING OR INSPECTION WILL RESULT IN DENIAL OR REVOCATION OF AUTHORIZATION TO BOARD OR ENTER 33CFR104.265(f)(3) 33CFR105.255(f)(3)

Conclusion
For questions, contact Sector Miami Port of Miami Field Office:
(786) 777-0775

24hr Duty Phone:
(786) 295-8995