Maritime Transportation Security Act (MTSA) Tips White Paper

ADT Advanced Integration

Introduction

As one of the oldest post-9/11 regulatory security programs, the Maritime Transportation Security Act (MTSA) program continues to evolve, and it is important for the regulated community to remain informed regarding recent and forthcoming MTSA guidance and programmatic adjustments. This paper is intended to provide helpful tips as well as updates on the current state of the MTSA and Transportation Worker Identification Credential (TWIC™) programs.

TWIC Program

TWIC is a security initiative established by MTSA to control unescorted access to "secure" areas of MTSA facilities. Initially deployed in 2008, the TWIC program is now in effect at 361 ports, 3,200 facilities and 14,000 vessels, and to date, more than 1.8 million cardholders are enrolled in the program. The TWIC itself is a standardized, tamper-resistant photo credential containing several physical security features that, when utilized, can provide a high assurance that the TWIC being presented is valid and that the holder is the same individual to whom the TWIC was issued. However, because the Coast Guard has yet to require the use of TWIC readers, most facilities have been unable to utilize the full security benefits of the TWIC.

TWIC™ Reader Pilot Program

Although the MTSA statute does not specifically require the use of TWIC™ readers, the Security and Accountability for Every Port Act of 2006 (the SAFE Port Act) made clear that Congress intended the use of TWIC readers to leverage the full security benefits of the TWIC. The SAFE Port Act created new statutory requirements for the TWIC program, including the development of a TWIC Reader Pilot Program to test the viability and operational impact of TWIC readers in the maritime environment, and the use of that data to develop a TWIC reader rule making. Eventually, following the passage of a TWIC reader rule, all MTSA-regulated facilities will be required to utilize TWIC readers.

During the initial TWIC Reader Pilot Program in 2008, the Coast Guard deployed approximately 250 TWIC readers at participating facilities and vessels throughout the United States. In March 2009, the Coast Guard published an Advanced Notice of Proposed Rule Making (ANPRM) regarding TWIC reader requirements. The ANPRM proposed using a risk-based model in which MTSA-regulated facilities and vessels would be separated into one of three risk groups, each with its own electronic TWIC reader requirements. Under this framework, higher-risk facilities and vessels would be required to fully utilize the TWIC's security features and achieve the full risk reduction benefit of the TWIC, whereas lower-risk facilities and vessels would be required to implement only some of those security features.

The TWIC Reader Pilot Program concluded in the summer of 2011. With information from the Pilot Program in hand, the Coast Guard is now compiling a report for submission to Congress. However, it appears that a TWIC Reader Notice of Proposed Rule Making (NPRM) will not occur until 2012.

TIP — Ensure you select a TWIC reader included on the Coast Guard's Initial Capability Evaluation (ICE) list.

The ICE list identifies TWIC readers that have been tested by the Coast Guard and Transportation Security Administration (TSA) and have successfully demonstrated the capability to read and process TWIC information.

TWIC™ Reader Pilot Program cont.

TIP — Before purchasing TWIC readers and/or other security equipment, try to seek grant funding.

Many facilities have been able to take advantage of the Federal Emergency Management Agency's Port Security Grant Program to implement and/or upgrade access control measures, such as approved TWIC readers. The Port Security Grant Program was established in 2002 under the MTSA statute to provide funding for port-related transportation security activities. In 2011, over $235 million was earmarked for distribution under the Port Security Grant Program. When considering integration partners to help select and implement security enhancements, such as those funded under the Port Security Grant Program, it is important to select a vendor which has been awarded SAFETY Act status by the Department of Homeland Security (DHS). Products and services that have been awarded Qualified Anti-Terrorism Technology (QATT) status (a process that results in either SAFETY Act Designation or Designation and Certification by DHS) may offer MTSA-regulated facilities additional liability protections, if an act of terrorism were to occur at the facility.

TWIC Control and Effectiveness Issues

Though the TWIC program has made significant progress in restricting access to MTSA facilities, a number of vulnerabilities still exist. In May 2011, the Government Accountability Office (GAO) released a report identifying internal control weaknesses governing the enrollment, background checking, and use of TWICs that it found may potentially limit the program's ability to provide reasonable assurance that access to "secure" areas of MTSA-regulated facilities is restricted to qualified individuals. GAO investigators conducted covert tests at several selected ports and were successful in gaining access "… using counterfeit TWICs, authentic TWICs acquired through fraudulent means, and false business cases (i.e., reason for requesting access)."

There have also been reports of individuals acting as TWICs "for hire." A TWIC "for hire" is a person with a TWIC who is paid a fee by a non-TWIC holder (e.g., a truck driver) to serve as a TWIC escort for access into a "secure" area of an MTSA facility. Though the Coast Guard has not issued any guidance regarding TWICs "for hire," some ports have attempted to limit their use by issuing a complete ban on the practice. Even without a port-issued ban however, individual facilities can curb the use of TWICs "for hire" by ensuring that each person granted access has a legitimate business need to enter the facility.

In July 2011, the TSA began using a new version of the TWIC. Other than a change in version number and date on the back of the card, there are no visible differences between the new card and the previous version.

TIP — The changes in the new version of the TWIC are only cosmetic; therefore, there is no need for current TWIC holders to obtain an updated TWIC.

However, facility and vessel security personnel should be aware of this change to assist in the recognition of authentic TWICs and in the detection of fraudulent TWICs. The Coast Guard continues to emphasize the need for facilities to remain vigilant in the verification of TWICs upon entry into a TWIC-affected area of a facility.

MTSA II

The MTSA regulations (33 CFR Part 101–106) have not been updated since their initial development eight years ago. The Coast Guard continues to work toward updating the MTSA regulations (MTSA II), but the agency has been generally quiet about the details of the changes it intends to propose through a forthcoming NPRM.

In a recent semiannual regulatory agenda, the Coast Guard indicated that the MTSA II regulatory update "… would incorporate feedback received from industry stakeholders, Coast Guard field units, and the public since the original MTSA regulations came into effect in 2003." The Coast Guard also noted that the revised rules would also, among other things, "… update existing regulations regarding the areas of maritime security plans, facility and vessel security plans, and facility exercise requirements in the SAFE Port Act of 2006" as well as "establish security training standards…" and "address screening standards for port facilities and vessels…." The expected NPRM publication date is now mid-2012 (earlier Coast Guard reports stated that the NPRM could be published before the end of 2011).

NTAS Update

In April 2011, DHS announced that the National Terrorism Advisory System (NTAS) would replace the color-coded Homeland Security Advisory System (HSAS). Unlike the HSAS, NTAS Alerts are only issued when credible information is available and include a clear statement that there is either an Elevated or Imminent threat.

This change raised questions among MTSA-regulated facilities, which had used the Maritime Security (MARSEC) Levels, based on the color-coded HSAS, to direct enhanced security measures identified in their SSPs. To clarify some of the issues associated with NTAS-MARSEC alignment, shortly after the transition, the Coast Guard issued a communication indicating the following:

(1) All references to the HSAS in the MTSA regulations are now obsolete;

(2) The three MARSEC Levels will continue to be used, with MARSEC Level 1 continuing to represent the normal day-to-day security level; and

(3) If DHS issues an NTAS Alert (i.e., Imminent Threat Alert or Elevated Threat Alert), then the Coast Guard will adjust the MARSEC Level if appropriate based on the commensurate risk, any maritime nexus, and/or after consultation with DHS.

The communication also explained that with regard to approved Facility Security Plans (FSPs), there is no requirement at this time to link the new NTAS with MARSEC Levels within individual FSPs. However, the Coast Guard expects that HSAS references (which currently exist in many FSPs) will be updated to reflect the NTAS as part of the normal amendment process or after the FSP's five-year renewal. Additionally, though the Coast Guard will not require facilities to link the new NTAS with MARSEC Levels on signage immediately, it does expect existing MARSEC signage posted at MTSA facilities to be adjusted expeditiously to reflect the change, as deemed appropriate by the facility.

CFATS-MTSA Harmonization

There has been much discussion among industry and government officials regarding the differences (and burdens) associated with the MTSA and Chemical Facility Anti-Terrorism Standards (CFATS) programs. Currently, MTSA facilities are statutorily exempt from CFATS. However, in July 2010, the DHS's Infrastructure Security Compliance Division (ISCD), which is primarily responsible for CFATS compliance, announced that it reached an agreement, *in concept,* with the Coast Guard to require some MTSA-regulated facilities to complete and submit CFATS Top-Screens. Though MTSA-regulated facilities are currently exempt from CFATS by law, this agreement comes as part of a coordinated effort between the Coast Guard and ISCD to "harmonize" chemical security regulations.

To compare aspects of the two regulations at the facility level, ISCD and Coast Guard officials visited an MTSA facility and then immediately visited a CFATS facility in the same geographic area. The CFATS-MTSA Working Group continues to conduct joint visits to CFATS and MTSA-regulated sites to compare the application of the two security programs side by side. Additionally, the Coast Guard and the ISCD have implemented inspector cross-training courses; for example, a CFATS briefing has been incorporated into the Coast Guard's Waterfront Facility Inspector's Course. The Coast Guard has also indicated that it has initiated the development of an NPRM requiring certain MTSA-regulated facilities to submit a Top-Screen. The agency has given no indication regarding the time frame for the publication of the NPRM, or how it intends to use the submitted Top-Screen information.

MTSA Guidance

TIP — Consult Coast Guard guidance documents when developing and/or updating your facility's FSP.

The Coast Guard issues periodic Navigation and Vessel Inspection Circulars (NVICs) to provide guidance on emerging MTSA and TWIC matters. NVICs are not legally binding but provide important information that helps facilities and vessels comply with the MTSA regulation. More frequently, however, the Coast Guard's MTSA/TWIC Policy Advisory Council (PAC) publishes short bulletins that clarify specific MTSA/TWIC implementation and compliance policy issues. These PAC decisions are available on the Coast Guard's Homeport website.

Sensitive Security Information

TIP — Remember that certain MTSA-related information is considered Sensitive Security Information (SSI) and must be protected as such.

SSI is a category of sensitive, but unclassified, information that must be safeguarded and protected from unauthorized disclosure. As it relates to MTSA, SSI includes, among other things, FSPs, Facility Security Assessments (and the corresponding Form CG-6025 which must be submitted with the FSP), MTSA training materials, and required MTSA records such as records of security threats and security drills and exercises. For additional information on SSI compliance, please view NVIC 10-04: Guidelines for Handling Sensitive Security Information (SSI).

Coast Guard Inspections

TIP — Ensure that you maintain records and documentation of all MTSA-related activities to present to the Coast Guard during a facility inspection.

Though the scope and frequency of Coast Guard MTSA inspections may vary across Captain of the Port zones, inspectors will generally be checking to ensure that the facility is complying with the provisions of its FSP. Inspectors will almost undoubtedly ask to see documentation and records of required security drills and exercises, security training and security incidents. They may also want to verify that appropriate signage is posted and unobstructed (i.e., Restricted Areas are clearly placarded and marked), and that appropriate access control measures are in place (TWICs are being checked prior to granting facility access, security gates are closed when not in use, etc.).

Conclusion

The MTSA and TWIC programs continue to evolve — both as regulatory programs in their own right and in the context of new challenges, such as harmonization with CFATS. Indeed, one thing is certain: these security programs are here to stay and will likely require more technical knowledge and commitments of time and resources in the coming months and years.

Additional Resources

Coast Guard Homeport: www.homeport.uscg.mil

TSA's TWIC Homepage: www.tsa.gov/twic

About ADT® Advanced Integration

ADT® Advanced Integration has a Petro-Chem & Energy Solutions group dedicated to serving the petrochemical industry. This team has petrochemical **security experience predating 9/11, MTSA and CFATS**, and has the knowledge to help deliver solutions in support of these regulations. In addition, each team member is a certified CVI (Chemical-Terrorism Vulnerability Information) Authorized User and can help companies develop and establish total security management plans for perimeter detection systems, video surveillance and access control. ADT Advanced Integration provides the following services: system consultation, project management and coordination, system installation and commissioning, general construction, system training, and maintenance and service. Plans are implemented with a practical approach to help configure an integrated security solution that is efficient and cost-effective.

ADT Security Services, Inc. ("ADT") is a unit of Tyco International and part of ADT Worldwide, the world's largest electronic security provider. In North America, ADT provides electronic security services to nearly 5 million commercial, government and residential customers. ADT's total security solutions include intrusion, fire protection, video systems, access control, critical condition monitoring, home health services, electronic article surveillance, radio frequency identification (RFID) and integrated systems. ADT's government and commercial customers include a majority of the nation's *Fortune* 500 companies, all U.S. federal courthouses and over 70 mid-to-large airports. Headquartered in Boca Raton, Florida, ADT has more than 24,000 employees at approximately 240 locations in the U.S. and Canada. ADT's services go beyond the installation of security systems. ADT is **SAFETY Act certified and designated** for Electronic Security Services from the U.S. Department of Homeland Security.

ADT Advanced Integration

For more information about chemical and energy solutions from ADT Advanced Integration, please call **888.446.7781**, or visit **www.ADTbusiness.com/petrochem**

L8714-00 (10/11)