

TranSystems Florida Seaport Security Assessment 2010

Contract No. 10-DS-20-14-00-22-087

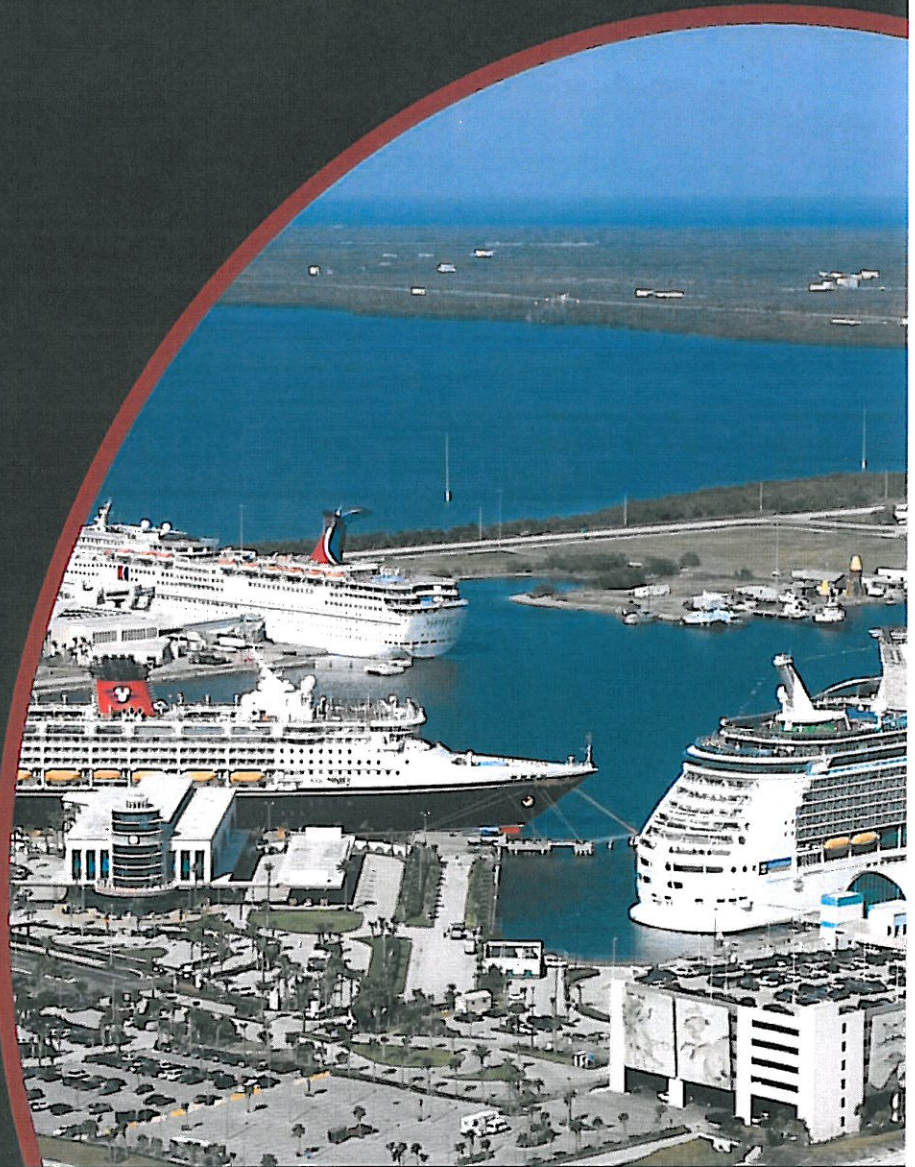
February 2010

Prepared for:
Florida Office of Drug Control

PREPARED BY:

TranSystems

TranSystems



Page Left Blank Intentionally

TranSystems Florida Statewide Seaport Security Assessment 2010

The opinions, findings, and conclusions expressed in this publication are those of the authors and do not necessarily reflect those of the state of Florida Division of Emergency Management or the Office of Drug Control.

Technical Report Documentation Page

| | | | | | |
|---|--|--|--|--|--|
| 1. Report No. N/A | | 2. Government Accession No. N/A | | 3. Recipient's Catalog No. N/A | |
| 4. Title and Subtitle TranSystems' Florida Seaport Security Assessment 2010 | | | | 5. Report Date February 2010 | |
| | | | | 6. Performing Organization Code NA | |
| 7. Author(s) Kim Petersen, Frank Galloway, Clare Austin | | | | 8. Performing Organization Report No. NA | |
| 9. Performing Organization Name and Address TranSystems Corporation 2400 E. Commercial Blvd Suite 1000 Fort Lauderdale, FL 33308 (954) 653 4700 kepetersen@transystems.com, ftgalloway@transystems.com, csaustin@tranSystems.com | | | | 10. Work Unit No. (TRAIS) NA | |
| | | | | 11. Contract or Grant No. 10-DS-20-14-00-22-087 | |
| 12. Sponsoring Organization Name and Address Florida Division of Emergency Management Florida Office of Drug Control 2555 Shumard Oak Boulevard Tallahassee, FL 32399 | | | | 13. Type of Report and Period Covered Final Report February 2010 | |
| | | | | 14. Sponsoring Agency Code 10-DS-20-14-00-22-087 | |
| 15. Supplementary Notes None | | | | | |
| 16. Abstract Prior to the passage of the Maritime Transportation Security Act (MTSA) in 2002, the state of Florida was extremely proactive in securing its deepwater ports with the passage of Florida Statute [FS] 311.12 Seaport Security Standards in 2000. This research explores the history, impact, and areas of overlap that FS 311.12 and the MTSA security standards have upon Florida's major seaports. The research includes: 1) an historical analysis of the 1999 <i>Camber Report</i> ; 2) a federal and state statutory regulation comparison; 3) a review of the Seaport Security Standards Advisory Council 2008 recommendations & FS 311 review; 4) U.S. port security regulatory review 2000-2009; 5) a comparison of aviation and maritime security regulations; 6) state and federal regulation evaluation – Layered Security; 7) a document review to analyze Florida ports' physical security and operations; 8) a combined Florida risk assessment update; 9) an analysis of the security costs incurred by Florida's ports vs. comparable ports that are not required to meet a state port security standard; and 10) an overlap analysis of the Florida Uniform Port Access Credential (FUPAC) against the Transportation Workers Identification Credential (TWIC). The report contains findings and recommendations associated with each of the listed tasks. | | | | | |
| 17. Key Words FS 311.12, MTSA, Florida Seaport Security, FDLE, USCG, FPC, ODC | | | | 18. Distribution Statement Do not distribute | |
| 19. Security Classification (of this report) Sensitive Security Information. | | 20. Security Classification (of this page) Unclassified. | | | |

Acknowledgements

TranSystems and the authors of this study would like to acknowledge the contributions of the following organizations without whose assistance this report would not be possible:

- Florida Division of Emergency Management
- Florida Office of Drug Control
- Florida Department of Law Enforcement
- United States Coast Guard
- U.S. Customs and Border Protection
- Florida Law Enforcement Agencies — Sheriff's & Police Departments
- Florida Ports Council
- JAXPORT
- Canaveral Port Authority
- Port of Fort Pierce
- Port of Palm Beach District
- Port Everglades
- Port of Miami
- Port Manatee
- Port of St. Petersburg
- Tampa Port Authority
- Port of St. Joe
- Port Panama City
- Port of Pensacola
- Port of Fernandina
- P.J. Murray Associates, Inc.
- Infrastructure Security Solutions LLC
- Maritime Directions Management Corp.
- Phelps Dunbar LLP

Page Left Blank Intentionally

Table of Contents

| | |
|--|------|
| Executive Summary | vii |
| 1.0 Analysis of the 1999 Camber Report's Legacy | 1-1 |
| 2.0 Federal and State Statutory Regulation Comparison..... | 2-1 |
| 3.0 Seaport Security Standards Advisory Council Report & associated changes to FS 311 Review | 3-1 |
| 4.0 U.S. Port Security Regulatory Review: 2000 & 2009 | 4-1 |
| 5.0 Aviation and Maritime Federal Regulations Comparison | 5-11 |
| 6.0 State and Federal Regulation Evaluation | 6-1 |
| 7.0 Combined Florida Physical and Operational Vulnerability Analysis..... | 7-1 |
| 8.0 Combined Florida Ports Risk Assessment Update | 8-1 |
| 9.0 Florida Ports Security Operations Costs Analysis..... | 9-1 |
| 10.0 TWIC FUPAC Analysis | 10-1 |
| 11.0 Annexes | 11-1 |

Page Left Blank Intentionally

Executive Summary

Introduction

On October 6, 2009, TranSystems Corporation was contracted by the Florida Office of Drug Control to provide an analysis of Florida's seaport security, and potential conflicts that exist between regulatory obligations mandated by the state under Florida Statute (FS) 311.12¹ and the federal government through the Maritime Transportation Security Act (MTSA) of 2002. Over a 100-day period, the TranSystems team conducted an exhaustive study that has resulted in this report.

The TranSystems team developed a comprehensive set of findings presented within the various sections of this study. These findings were based on the analyses of state statutes, federal regulations, seaport security documents, survey data gathered specifically for this report, criminal incident reports, open source and classified threat intelligence, and interviews with government and private sector stakeholders.

Background

Prior to 2001, studies by the federal government and the Florida Department of Law Enforcement (FDLE) determined that Florida's seaports were conduits for a variety of criminal activities, including drug smuggling, money laundering, and other criminal conspiracies. Significant contributing factors to this phenomenon were the vulnerabilities in physical, personnel, and information security at Florida's seaports. To address these concerns, in 2001, Florida achieved a significant milestone through its passage of FS 311.12. This new law mandated minimum security requirements including seaport security plans, security training, fencing, lighting, access controls, and other security measures. Inasmuch as FS 311.12 falls under Chapter 311 *Florida Seaport Transportation and Economic Development*, it is clear that the framers of this legislation were cognizant of the importance of Florida's seaports to the state's economy.

As a result of the terrorist attacks of September 11, 2001, the U.S. implemented wide-ranging regulatory measures and guidelines specifically targeted at protecting the nation's seaports. The federal government's multi-layered security strategy is deployed across several agencies that have responsibilities for transportation security, including the Department of Homeland Security (DHS), Transportation Security Administration (TSA), U.S. Customs and

¹ FS 311.12 falls under Section 311 of Florida State law entitled *Florida Seaport Transportation and Economic Development*.

Border Protection (CBP), and the U.S. Coast Guard. When FS 311.12 was introduced by Florida's Legislature, it could not have envisioned the events of 9/11 or the assumption of responsibility for seaport security by the federal government almost a decade later. Following the enactment of the MTSA, *Florida is the only state with its own statutory seaport security regulations.*

However, with the adoption of the MTSA, along with the SAFE Port Act of 2006 and other related federal seaport security regulations, guidelines, and port security grant programs, Florida's seaport community has asked whether FS 311.12 is still necessary. Many argue that duplication, overlap, and conflict exist between the regulatory obligations directed at seaport operators within FS 311.12 and MTSA. One of the central concerns raised by the private sector is the degree to which two sets of security standards and obligations create a competitive and economic disadvantage for Florida's seaports with respect to neighboring states. If true, this could have far-reaching consequences on what are called "the economic engines" for Florida's economy – the state's 14 deepwater seaports. To underscore their importance, it is revealing that in 2008 maritime cargo activities at these seaports were responsible for generating more than 550,000 direct and indirect jobs and \$66 billion in total economic value.

Recommendations

The following is a brief summary of key findings followed by our recommendations; complete findings and analyses associated with the recommendations are found later in this report. It should be noted that these recommendations do not necessarily reflect the point-of-view of every stakeholder that participated in our research. Indeed, it is likely that no party will agree with every recommendation that we put forth. However, these recommendations are consensus driven from a team that contains national experts in maritime security, including former law enforcement officials, intelligence officers, seaport directors, maritime security educators, maritime and aviation security specialists, U.S. Coast Guard personnel, and port security directors.

Key Findings

1. FS 311.12 was a necessary and important step in addressing identified threats arrayed against Florida's seaports at the time of its passage — and it built a strong foundation for later compliance with the MTSA.
2. As a consequence of FS 311.12 and the early efforts of FDLE, Florida's seaports are better prepared to deter, detect, delay and

deny both criminal and terrorist threats than ports in any other state.

3. FDLE was an essential partner to the seaports in ensuring that physical, personnel, and information security programs were instituted statewide prior to the enactment of MTSA.
4. As a consequence of 9/11, and the subsequent passage of the MTSA, the federal government has created regulations that have effectively and capably rendered much of FS 311.12 obsolete. For example, both MTSA and FS 311.12 regulate and / or provide for seaport security plans, practices, and audits.
5. The MTSA obligates Florida's seaport security directors to create and update on an ongoing basis a threat and vulnerability assessment for their respective ports. Such assessment is then used to develop a Facility Security Plan (FSP) containing port-recommended risk mitigation measures subject to U.S. Coast Guard approval. This is extremely difficult for them to accomplish in a professional manner given the lack of available threat intelligence resources to these security directors. Their only available threat intelligence is general in nature, and found through open source material or on the U.S. Coast Guard's HOMEPORt web site. Absent port-specific international, regional, and local threat intelligence, seaports are left to speculate as to the risk they are obliged to mitigate.
6. The existence of dual regulations – by both Florida and the federal government – has created confusion, duplication of effort, and wasted financial and human resources, all of which could be put to better use enhancing seaport security. As an example, FS 311.12 requires FDLE to conduct seaport security compliance audits while the MTSA also requires the U.S. Coast Guard to conduct compliance audits of the same ports. This creates an obvious duplication of effort and waste of resources.
7. By reference, FS 311.12 prescribes physical standards that are neither performance- nor risk-based. This has resulted in the expenditure of substantial financial resources to protect, for example, empty fields and aggregate storage yards that pose no risk to the seaport or the surrounding community. While a waiver process does exist, ports have reported that it is burdensome, time consuming, and costly. "Best practices" that are utilized in Florida, and throughout the U.S., typically refrain from *prescribing* security standards, and instead employ flexible *performance* standards that are based on risk.
8. Prior to MTSA, Florida instituted a much-needed port ID program that required a background check performed by FDLE. Subsequent to the enactment of the MTSA, the federal government created the Transportation Worker Identification Credential (TWIC) which requires the applicant to be fingerprinted and a background check be performed by the FBI prior to its issuance. All persons requiring access to restricted areas of a seaport in Florida must now hold a TWIC. However, FS 311.12 requires that seaports continue to perform state background checks and collect fees from TWIC-holders. Florida is believed to be the only state that requires both a federal *and* a state background check. Florida's seaport directors

and tenants point to this requirement as an expensive and cumbersome legacy element of FS 311.12. The federal government believes that the background checks performed by TSA, and using the FBI's criminal database prior to the issuance of a TWIC, are sufficient to protect seaports against the introduction of individuals who could pose a threat.

9. The Seaport Security Standards Advisory Committee (SSSAC) membership, as authorized by Florida's Legislature, is not reflective of the stakeholder community it is designed to serve. At present, nine of 13 positions are dedicated to state government representatives. The U.S. Coast Guard does not hold a permanent seat on the committee. Furthermore, the SSSAC is not required to produce an annual report to the Governor or Legislature on the status of seaport security within the state.
10. The *Port Security Standards — Compliance Plan* (2001), which is incorporated by reference in FS 311.12, requires that seaports employ sworn law enforcement officers. This results in a highly trained and costly police force performing routine security functions, such as credential checking at access points and security patrols that are typically conducted by contract security personnel at seaports elsewhere in the U.S. This requirement exists even if the seaport can demonstrate that local police or sheriff's personnel are able to respond in a timely manner to an emergency within the port. It also does not take into consideration that, subsequent to the enactment of the MTSA, there is often a federal presence within the port, including agents from CBP and Immigration and Customs Enforcement (ICE), as well as U.S. Coast Guard personnel. While such federal officials may not have a police function *per se*, they do serve as a strong deterrent against crime. This requirement is one of the most costly obligations required by FS 311.12.
11. Data collected in this study demonstrates that higher operating costs associated with dual regulations have severely impacted seaport operating budgets, resulting in reduced infrastructure improvements, a loss of jobs, and diminished competitiveness with neighboring states.

Recommendations

TranSystems recommends that rather than continuing the struggle to 'align' FS 311.12 with the MTSA, the Florida Legislature consider implementing these recommendations:

1. **USCG Regulation of Port Security:** Recognize the authority vested to the U.S. Coast Guard and Captain of the Port (COTP) by the federal government, and transfer sole responsibility for security standards, plans, practices, and audits to the U.S. Coast Guard. The U.S. Coast Guard and the COTP should exclusively perform seaport security compliance inspections and audits.
2. **FDLE Port Security Role:** Re-task FDLE with the responsibility to develop and promulgate port-specific threat intelligence (e.g., international, national, state, & local) for use by seaport security directors in the fulfillment of their MTSA-obligation to conduct ongoing threat and vulnerability assessments of their seaports. Ensure that appropriate funding is provided to FDLE for this role, which will substantially increase the manpower requirements that they are currently allocated for seaport security. Eliminate FDLE's compliance inspection responsibility under FS 311.12.
3. **SSSAC Membership Modification:** Reconstitute the Seaport Security Standards Advisory Committee (SSSAC) membership to provide greater participation by Florida seaport stakeholders (e.g., seaport management, shipping companies, and seaport tenants). The Committee should meet at least quarterly, and issue an official report on an annual basis to the Governor and the state Legislature on the "State of Seaport Security" for their review and possible action. The SSSAC membership should be composed of six state representatives, one representative from the U.S. Coast Guard, and six representatives from the private sector.
4. **Performance- and Risk-Based Security Standards:** Eliminate the prescribed security standards contained within the *Port Security Standards Compliance Plan* (2001) as referenced in FS 311.12. Florida seaports should incorporate performance- and risk-based security standards as required by 33 CFR Part 105 and that are subject to approval by the U.S. Coast Guard.
5. **State Background Check:** Abandon the requirement for state criminal background checks for individuals requesting access to restricted areas within Florida's seaports if they have successfully undergone an FBI-conducted background check and have been issued the federal TWIC.
6. **Port Access Control ID Badges:** Authorize seaports to issue a Port Access Control ID Badge for use at their respective port and stipulate that the Port Access Control ID Badge will be used in conjunction with TWIC. The issuance of a Port ID badge should be contingent upon:
 - Presentation of a valid TWIC;
 - Submission of a notarized *Document of Request for Issuance of a Port ID Badge* (DoR). Such document should be provided by a tenant, vendor, or other authorized party having business in the

port, and attesting to the need of the individual named within the DoR to access the port's restricted areas;

- Port Access Control ID Badges should contain the photograph and name of the bearer, the name and emblem of the port, area(s) of authorized access, and a date of expiration matching that of the bearer's TWIC; and
 - Ports should be authorized to charge a fee to cover the related administrative costs.
7. **Sworn Law Enforcement Presence Requirement:** Eliminate the legislative requirement for an on-site sworn law enforcement presence at the ports. Ports that choose not to have on-site law enforcement should be required to demonstrate the ability of the local sheriff or police department to respond within a reasonable time to an emergency. Seaports shall engage licensed contract security personnel, law enforcement officers, or a combination thereof to perform access control, screening, patrols, and other security functions stipulated within their FSP and approved by the U.S. Coast Guard COTP.

Conclusion

While there were numerous obstacles in the development of this report – including continual delays in receiving essential data and not receiving requested data at all – this report provides a comprehensive analysis of the current port security regulatory environment in the state of Florida. The above findings and recommendations, and the detailed report to follow, was prepared to provide the Florida Office of Drug Control a clear understanding of the challenges Florida's ports face in complying with two redundant regulations. The intent of this report is to highlight the recognized deficiencies and offer cost-effective solutions to enhance the security of Florida's seaports.

Despite the impediments faced in preparing this report, TranSystems received sufficient information and commendable assistance from all the necessary stakeholders – especially from the seaports, FDLE, U.S. Coast Guard, and the Florida Ports Council – such that we are confident the content within will meet this report's intended goal.

1.0 Analysis of the 1999 Camber Report's Legacy

1.1 Introduction

Prior to passage of Florida Statute 311.12 (FS 311.12) or the Maritime Transportation Security Act (2002), a comprehensive review of the nature and extent of seaport crime, and the overall state of security in U.S. seaports was conducted by a task force of federal government agencies. The resulting report, issued in 2000 by the Federal Interagency Commission on Crime and Security in U.S. Seaports, rated the state of security in U.S. seaports from "poor to fair," and identified a prioritized list of the major threat categories against which the ports needed to be protected. The Commission found that Florida was attractive to drug traffickers due to the state's geographic proximity to drug source countries, along with its numerous international airports and deep water seaports.

Subsequent to the release of the federal government's report, the Executive Office of the Florida Governor's Office of Drug Control commissioned a statewide security assessment to identify the credible threats and associated risks to Florida's seaports. The assessment included an evaluation of the credible threats to Florida's seaports, and the results of on-site observations and findings of the security infrastructure and operations at each of Florida's public ports. The observations conducted and the subsequent findings addressed a number of specific security issues and challenges, including but not limited to:

- Complexity of Seaport Operations;
- Lack of Current Security Standards;
- Differing Definitions of Security;
- Threat Information & Crime Data;
- Interagency Coordination;
- Vulnerability to Terrorism;
- Standing Security Committees;
- Responsibility for Seaport Security;
- U.S. Coast Guard's Role in Seaport Security;
- Fundamental Elements of Seaport Security;
- Law Enforcement Presence at Florida's Seaports;
- Preferred Means of Maritime Smuggling;
- Money Laundering;
- Cruise Line Security and Security of Cruise Operations;
- Use of Non-Intrusive Inspection Technology at Florida Seaports;
- Compatibility of Technology and Operational Requirements;
- and
- The Miami River.

The resulting document, known as the *Camber Report*, provided recommendations to Florida's Legislature for the development of a state statute to address the myriad security issues identified, and to deter, detect, or respond effectively to criminal and terrorist activities at Florida's commercial seaports. The recommendations included the following:

- Adopt prescriptive minimum standards for all seaports;
- Establish a seaport agency accountable for security planning and execution;
- Implement appropriate limitations on individuals with access to seaports; and
- Provide independent oversight of seaport security activities.

In response to the *Camber Report's* recommendations, the Florida state Legislature promulgated FS 311.12, which established the legislative imperative for the development of statewide minimum seaport security standards for application at specifically identified public seaports in Florida; established policies and procedures for the determination of persons who may be allowed unescorted access into port restricted areas; and identified the Florida Department of Law Enforcement (FDLE) as the executive agent for the evaluation of compliance with the statute's minimum security standards at the identified Florida ports.²

Our review of the *Camber Report* evaluates to what extent FS 311.12 successfully achieved the objectives recommended in the report, and to what degree FS 311.12 remains a necessary regulatory instrument to reduce the risk of criminal or terrorist incidents at Florida's commercial seaports. To this end, the following issues are evaluated against the standards, security objectives, and performance measures identified in FS 311.12 (2009):

- Current and evolving threats to Florida seaports;
- Impact of FS 311.12 security measures on credible threats;
- Impact of federal security regulations on Florida's Seaports; and
- The economic consequences of maintaining duplicate security standards and practices.

1.2 Analysis of Evolving Threats

The *Camber Report* provided the Florida Legislature with a snapshot of the status of credible threats present at Florida's commercial seaports. At the time the *Camber Report* was developed, drug smuggling, cargo theft, internal conspiracies, money laundering, and smuggling of illegal

² FS 311.12 (4)(c) designated that, beginning with the 2001 – 2002 fiscal year, "the Florida Department of Law Enforcement (FDLE) or any entity designated by the department, shall conduct no less than one annual unannounced inspection of each seaport listed in s. 311.09 to determine whether the seaport is meeting the minimum standards established pursuant to this section...."

immigrants into the U.S. via commercial maritime vessels were the primary credible active threats at Florida's seaports. The threat of terrorist activity, either transiting or directed at Florida's seaports, was considered possible but was ranked lower in probability.

The *Camber Report's* threat assessment included a review of open source literature, which identified trafficking in cocaine through the state's maritime domain as the predominant illegal activity. The report identified the state as a focal point of regional counter-drug efforts due to the Florida's approximately 1,350 miles of largely unprotected continental coastline, and its status as home to four of the country's busiest container ports and three of the world's top passenger cruise ports.

Per the *Camber Report*, Florida's seaports operate within a complex intermodal transportation system. Seaport security needed to be considered in the context of that system. The report also noted that seaport management was not well informed about the current and evolving threats faced by their ports relative to cargo theft, drug smuggling, or terrorism. The lack of seaport threat, vulnerability, and risk assessments – combined with the lack of a mechanism for the timely provision of accurate threat intelligence for early threat assessments, planning, and response decisions – severely limited the ability of Florida ports to execute a coordinated response to any real or perceived criminal or terrorist events.³

Four of Florida's ports were regarded as "high-risk" facilities based on the perceived threats to their facilities and commercial activities, and were identified as requiring the application of measures to maximize security preparedness against those threats. Six ports were regarded as "medium-risk" facilities, warranting moderate security preparedness, and four others were regarded as having "low-risk" facilities and operations. This categorization of risk, based on an evaluation of the vulnerability of these ports and the impact of the threats against their operations, was used as a basis for the prioritized allocation of resources for implementation of risk reduction measures.

In the ten years since the release of the *Camber Report*, the threat profiles at Florida's ports have changed. The implementation of preventive security measures, including the federal requirement for background screening of persons requesting access to seaports; the use of non-intrusive screening devices for personnel, vehicles, and cargo; and, a heightened federal presence, has resulted in the reduction of illegal narcotics into Florida via the methods prevalent in 1999. However, as a result of the deliberate targeting by terrorists of transportation and

³ Information regarding landside security threats or incidents, such as targeting of containers of high value merchandise, was not readily available or transmitted to port management to support their planning and implementation of protective security measures.

supply chain infrastructure, and operations, the risk of a terrorist act at Florida's seaports has increased during the same period.⁴

1.3 Federal Security Regulations Impact on Florida's Seaports

The implementation of a statute that applied minimum security standards for uniform application at commercial seaports placed Florida in the national forefront in the identification and protection of critical transportation infrastructure. The events of 9/11, however, highlighted the vulnerability of our nation's ports and the federal government subsequently passed the Maritime Transportation Security Act (MTSA) of 2002, which created the following security standards and performance objectives for all commercial seaports in the U.S.

- Identify requirements for maritime security professionals responsible for security planning, management, and operations at commercial U.S. seaports and applicable marinas, on U.S. - flagged and foreign commercial vessels calling at U.S. seaports; and with companies engaged in commerce via MTSA-regulated seaports;
- Development of a Facility Security Plan (FSP) that is based on a threat and vulnerability assessment of the facility and its operations, and that identifies the security infrastructure, plans, personnel and operations to detect, deter, or respond to those identified credible threats;
- Development of a program for security training, drills, and exercises to reinforce the effective implementation of the security policies and procedures outlined in the FSP;
- Establishment of the U.S. Coast Guard as the executive agent for oversight and enforcement of MTSA security standards; and
- U.S. Coast Guard management of a program for the collection, analysis, and timely dissemination of credible threat information to support the planning and execution of effective security incident notification, response, and recovery actions.

1.4 Dual or Dueling Standards?

Upon implementation of the MTSA, Florida's ports were placed in the position of having to comply with two sets of standards and practices. While the intent of both the state and federal regulations is to create a secure operating environment for commerce at commercial seaports in Florida, the standards and associated processes for implementation and

⁴ Terrorist attacks on transportation infrastructure around the world, as well as the capture of terrorist training manuals in the U.K. describing the processes for conducting surveillance on ports and intermodal facilities – including documented incidents of these types of activities directed at a Florida seaport – clearly validates the increase of terrorism as a credible threat against Florida's seaports.

compliance differ greatly. The differences have resulted in Florida's ports operating under competing security imperatives, such as:

- **Prescriptive Standards of FS 311.12:** FS 311.12 security standards are prescriptive and detailed, and the focus is on the ports' rigid adherence to the letter of the standard (e.g., the level of illumination at port areas categorized as "restricted" must be five (5) foot candles);
- **Performance and Risk-Based MTSA Standards:** MTSA security standards are performance-based. MTSA standards are also modifiable according to the risk associated with the threat. For example, the level of illumination at port areas categorized as "restricted" must be appropriate to the identified threat. Layered security measures may be applied to achieve the required level of protection for the materials or operations protected;
- **Equivalency Waivers:** FS 311.12 (2009) includes a process for requesting equivalency waivers for prescriptive security measures that must be submitted to the security standards committee for review, evaluation, and determination;
- **MTSA Compliance:** Compliance with MTSA's performance-based standards may be adjudicated by the local U.S. Coast Guard (USCG) Sector Commander based on the findings and recommendations of the USCG compliance audit inspection;
- **FS 311.12 Compliance:** The Florida Department of Law Enforcement (FDLE) is, by statute, the agency responsible for conducting audits of Florida ports' compliance with the standards established by the state Legislature;
- **State Threat Intelligence Assistance:** FDLE does not have a defined role to provide guidance or assistance to ports regarding compliance with FS 311.12, nor does it provide port-specific threat intelligence to seaport operators;
- **Federal Threat Intelligence Assistance:** The USCG provides generic threat information to Florida's ports but does not provide port-specific threat intelligence;
- **FS 311.12 State Background Checks:** FS 311.12 requires the conduct of criminal background checks against state-defined felony standards for issuance of a port-issued identification/access credential;
- **TWIC Background Checks:** The MTSA mandates the conduct of criminal background checks against federal standards for issuance of a Transportation Worker Identification Credential (TWIC) required for all personnel requiring access into ports that are subject to the federal statute; and
- **Standards Revision Process:** Florida's Statewide Minimum Seaport Security Standards may only be modified by the state Legislature to address changes in Florida Statute, as recommended by the Standards Committee to the Legislature.

Guidelines for implementation of the port security standards outlined in MTSA are provided in 33 CFR, part 105, and U.S. Coast Guard Navigation and Inspection Circular (NVIC) 03-03, Change 2, which may be modified as part of a federal rule-making process that allows for comments and recommendations from the port community.

FS 311.12 (2009) recognizes the changes that have occurred in the threat and regulatory environments subsequent to the promulgation of FS 311.12 (2001), and clearly identifies the state Legislature's intent to more closely align the state's security standards and performance objectives with federal standards and practices. Significant changes include, but are not limited to:

- Aligning state definitions of secure and restricted access areas within a seaport with federal definitions;
- Aligning state criminal offenses that disqualify a person for unescorted access to secure and restricted access area within a seaport with federal disqualifying offenses under the TWIC program;
- Allowing all or part of Florida's seaports identified in FS 311.09 to be exempted from the state seaport security standards if a determination is made that activities associated with such facilities are not vulnerable to criminal activity or acts of terrorism; and
- Establishing an equivalency waiver process for security standards identified in the Port Security Standards Compliance Plan, as long as security of the port facility or operations is not diminished as a result.

1.5 Analysis

Consequences of Non-Compliance: Non-compliance with MTSA ranges in fines (up to \$25K) to interruption of the port's commercial operations. Non-compliance with the more restrictive security standards of FS 311.12 results only in FDLE's notification to the state Legislature of the offending port's "non-compliance" with the statutory requirements. As a result, some of Florida's ports have been placed in a position of choosing to invest their limited financial resources towards compliance with federal standards and performance objectives instead of those mandated under the state statute.

Security Spending and the Point of Diminished Returns: Ports were consistent in reporting to us that the inflexible security measures required for compliance under the state statute provide no additional protection to the port against the identified credible threats. For example, the state's requirement for specified fencing, lighting, and access controls at waterside terminal facilities are required whether or not such facilities are at risk. For example, Florida's ports have been required to

implement expensive, and arguably, excessive security measures at areas where low-value and low-risk materials were stored (i.e., aggregate, scrap metal, etc.).

Two Background Checks: As previously stated, both state and federal maritime security regulations require criminal background investigations to be conducted – against different standards – to receive access credentials, both of which have fees associated with the mandated investigation. Interviews with port management and security personnel indicate that the collection of dual fees, to support what is widely viewed as a redundant requirement, is considered a mechanism for generating revenue for the state, and does not serve to enhance security at the seaports.

1.6 Conclusion

FS 311.12 (2001) mandated the implementation of minimum port security standards, which are set forth in the Port Security Standards Compliance Plan.⁵ Compliance with these prescriptive standards focused on each port's adherence to the letter of the requirements identified in the Office of Drug Control and FDLE-developed Port Security Standards Compliance Plan, and were applied and evaluated regardless of changes to each port's threat and risk profiles.

FS 311.12 (2009) successfully addressed many, if not all, of the concerns outlined in the *Camber Report* by maintaining minimum security standards for physical infrastructure, personnel, information resources, planning, and operations for application at all of Florida's commercial seaports identified, and addressed the establishment of mechanisms for the ongoing evaluation and dissemination of evolving threats to Florida's seaports. *Port security professionals were in near unanimous agreement that the fundamental problem they face is that FS 311.12 stipulates prescriptive security standards that fail to consider the specific threat and risk faced by their respective port.*

Inexplicably, the ports are required to conduct threat and risk assessments to satisfy FS 311.12 requirements, even though such assessments have no bearing on the security standards imposed on their ports. The 2009 modification to FS 311.12 allows for waivers from the standards based on assessment findings. However, industry 'best practices' typically apply security standards *subsequent* to the performance of a threat and vulnerability assessment; they do not impose standards first, followed by a threat and vulnerability assessment, and then require a burdensome waiver process to undo unreasonable standards.

⁵ Statewide minimum standards for seaport security applicable to seaports listed in FS 311.09 shall be those based on the Florida Seaport Security Assessment 2000 and set forth in the Port Security Standards Compliance Plan delivered to the Speaker of the House of Representatives and the President of the Senate on December 11, 2000.

FS 311.12 (2009) offers an opportunity for closer alignment between state and federal security standards and practices in order to create a secure operating environment for maritime commerce in Florida.

Interviews conducted as part of this study, however, indicate that many of Florida's ports do not fully understand the impact of the changes in FS 311.12 (2009) on their security policies, processes, and operations. In addition, many of the ports have not yet been subjected to an FDLE compliance audit against the security objectives identified in the Seaport Security Data Collection Uniform Guidelines for Field Inspection Activities.⁶ The success and continued existence of FS 311.12 as a viable statute will be dependent upon the state's ability to facilitate the education of Florida's ports on the positive impact of the changes in the statute.

⁶ The effective date for FS 311.12 was July 1, 2009, following which FDLE compliance audits were temporarily suspended to allow Florida seaports to review and implement the changes contained therein. Interviews with many of the ports indicate that they have not received guidance or assistance from FDLE on their expectations regarding the revised compliance audit process. One port that did receive a compliance audit based on the new guidelines indicated that they did not receive the new guidelines against which the FDLE audit was conducted until after the audit was conducted, and are currently revising their facility security plan to include the new guidelines.

2.0 Federal and State Statutory Regulation Comparison

2.1 Introduction

This study is intended as a comparative analysis of the most recent versions of the state and federal regulations that establish minimum security standards applicable to the following commercial seaports: Jacksonville, Fort Pierce, Palm Beach, Port Everglades, Miami, Port Manatee, St. Petersburg, Tampa, Port St. Joe, Panama City, Pensacola, Key West, and Fernandina.⁷⁸

We have also included research into the history, impact, and areas of overlap between FS 311.12 and the Maritime Transportation Security Act (MTSA) of 2002, and their associated guidelines for implementation. We have also identified issues relating to the construction and evolution of these regulatory requirements. FS 311 (Florida Seaport Transportation and Economic Development) provides the following specific guidance applicable to Florida's Seaports:

- **311.09:** Identifies commercial seaports that are subject to an audit by the Florida Department of Law Enforcement (FDLE) for compliance with state minimum security standards within the state of Florida;
- **311.12:** Establishes the statewide minimum standards for security applicable to the seaports identified in FS 311.09, as set forth in the Port Security Standards Compliance Plan of 2001;
- **311.13:** Identifies the information, that if released could jeopardize the security of the seaport, as exempt from disclosure;
- **311.115:** Establishes the creation, role, and responsibilities of the Seaport Security Standards Advisory Council (SSSAC);
- **311.121:** Identifies the criteria under which seaport security officers and other personnel certified under federal and state guidelines may detain persons for trespassing at a Florida seaport;
- **311.122:** Identifies authority for the creation of a seaport law enforcement agency, the creation of requirements for compliance with law enforcement certification standards, and the range of law enforcement powers that may be exercised by seaport law enforcement officers; and
- **311.123:** Identifies the requirement for creation of a maritime domain security awareness training program for all personnel employed within a seaport's boundaries and the implementation of each seaport's security plan.

Questions underlying the comparison between the state and federal

⁷ FS 311.09 does not include the privately-operated, commercial Miami River Seaport.

⁸ Interviews with personnel responsible for management of Port Ft. Pierce are managed by Indian River Terminals, a private entity, on behalf of the County Commission. In addition, operations at the Port of Fernandina are managed by its private tenant.

security regulations include:

- Does compliance with the FS 311 security standards create areas of overlap, redundancy, conflict or inefficiency with federal standards mandated by MTSA?
- Has compliance with both state *and* federal security standards imposed additional operational burdens on Florida's commercial seaports?
- Has compliance with two sets of security standards and practices resulted in impediments to commerce, including higher operating costs, at Florida's commercial seaports?
- What changes facilitate more effective alignment of state and federal seaport security standards and practices?

Exclusions to the Study

This study does not provide an analysis of the effects of implementation of MTSA security standards and procedures on the types and frequency of security incidents or criminal activities documented as having occurred at the Miami River Seaport.

Port of Fort Pierce: This small east coast Florida port has been included in the list of deepwater ports in FS 311.09(1). The port is officially listed and participates in the Florida Ports Council and Florida Seaport Transportation and Economic Development Council (FSTED) and complies with such requirements such as a Port Master Plan. However, the port area does not currently have any international cargo trade activity on publicly owned port property. FDLE chose to categorize Port of Fort Pierce as an "inactive port" from an operating standpoint and hence exempt from complying with the on-going seaport security activities of FDLE under FS 311.12.

Port of Miami River: The Miami River is the fifth largest port in the state of Florida, serving as economic catalyst for the South Florida region and providing vital shipping links to the shallow draft ports of the Caribbean and Central and South America. As a working river, the Miami River's navigation and commercial shipping directly generates millions of tons of cargo each year and thousands of direct and indirect jobs. Miami River cargo transshipment is estimated at \$4 billion per year. All of the shipping terminals operated from the Miami River are private property and were not included as a deepwater port under defining state legislation in FS 311.09 that gave the other Florida public deepwater ports status under law. Hence, the Miami River terminals are exempt from the state of Florida's seaport security legislation.

Assumptions & Expectations

The basic assumptions and expectations underlying the conduct and intent of this study are:

- The primary objective of both FS 311 and MTSA is to ensure a

-
- secure operating environment for maritime commerce in the State of Florida;
 - The implementation of regulatory security standards is designed to maximize the effectiveness of the Florida seaport community's efforts to prevent, mitigate, and/or recover from a broad range of security and criminal threats or activities;
 - Conflicts between the two regulatory regimes need to be addressed in order to develop an effective mechanism for their alignment in a cost- and operationally-effective manner; and
 - Implementation of security regulations at Florida's seaports must maintain a reasonable balance between security practices, port operations and costs in order to maximize the effectiveness of security measures without diminishing the commercial viability of the port and its operations.

Historical Background

In 1999, President Clinton called for a comprehensive review of the nature and extent of seaport crime, as well as the overall state of security in U.S. seaports. The resulting report, issued in 2000 by the Federal Interagency Commission on Crime and Security in U.S. Seaports, rated the state of security in U.S. seaports from "poor to fair", and identified a prioritized list of the major threat categories against which the ports needed to be protected (*Report of Interagency Commission on Crime and Security in U.S. Seaports, 2000*). The Commission found that Florida was attractive to drug traffickers due to the state's strategic position near drug source countries and its numerous international airports and deep water seaports.

Subsequent to that report, the Executive Office of the Florida Governor's Office of Drug Control commissioned a statewide security assessment to identify the credible threats and associated risks to Florida's seaports. This report, known as the *Camber Report* (See Section 1), became the basis for the development of FS 311.12 which identified security standards to prevent criminal activity and money laundering at Florida's commercial seaports. The statute identified the FDLE as the executive agent for oversight, with the authority to conduct annual compliance audits of the required seaport security standards under FS 311.12. Implementation of FS 311.12 predated the events of 9/11, and placed Florida to the forefront of national leadership in securing its commercial maritime infrastructure and operations.

The Maritime Transportation Security Act of 2002 (MTSA) was created following the successful terrorist attack of 9/11, and was designed to provide a mechanism for the effective protection of commercial maritime infrastructure and operations at U.S. seaports against a variety of terrorist and criminal threats. MTSA requires 'performance-based' standards designed to protect against credible threats at all regulated seaports in the U.S. The U.S. Coast Guard serves as the executive agent responsible for oversight and enforcement of the MTSA, and

promulgates directive guidance on the performance measures and standards required for compliance with the objectives identified in 33 CFR Part 105 (Facility Security). Annual MTSA compliance audits are conducted by U.S. Coast Guard personnel.

Subsequent to the nationwide implementation of the MTSA, Florida's commercial seaports, and their tenants, have struggled to comply with these two distinctly separate regulatory requirements. Although the state and federal regulations share the same intent, their approach and method for addressing evolving threats unique to each port – as well as the mechanisms for oversight – are dissimilar and sometimes conflicting. The additional measures and associated costs required to achieve concurrent compliance with both the state and federal requirements imposes a burden on Florida's commercial ports. The results in some cases are:

- Seaports opting to comply with federal standards only due to insufficient funding; and
- Seaports finding themselves at a competitive disadvantage with ports in neighboring states due to the high cost of complying with dual regulatory regimes.

Security Standards – Construction & Enforcement

FS 311.12 imposes standards for physical infrastructure, personnel security, and information security procedures and practices against which the identified seaports are evaluated for compliance. The FS 311.12 standards are prescriptive in nature, and provide detailed guidance regarding specifications, systems, materials, and construction.⁹

FS 311.12-regulated ports have historically been required to maintain compliance with the letter of the standards outlined in the statute, on a 'pass/fail' basis, without regard to:

- The type and volume of credible threats to the facility;
- The level of risk associated with the credible threats to the port facility;
- The relative value of the area or materials within the port to be protected;
- Additional, layered risk measures implemented by the facility;
- The presence of federal law enforcement agencies (i.e., CBP, ICE, USCG); or,
- The cost-to-value ratio of the preventive security measures mandated by the state statute.

The 2009 version of FS 311.12 requires seaports to adhere to security practices that are consistent with the risks identified during the quarterly

⁹ Statewide minimum standards for seaport security applicable to seaports listed in s. 311.09 shall be those based on the Florida Seaport Security Assessment 2000 and set forth in the Port Security Standards Compliance Plan delivered to the Speaker of the House of Representatives and the President of the Senate on December 11, 2000.

risk assessments required to be conducted by each port. FS 311.12 (2009) does not specify which assessment tools or methodologies are to be used, but recommends coordination with the U.S. Coast Guard for use of the Maritime Security Risk Assessment Model (MSRAM) tool to assist seaport directors in their assessment of the risk of terrorist activities at their seaports. It should be noted that under FS 311.12 the seaports must perform ongoing threat and risk assessments, despite their lack of access to meaningful threat data. Such data is often classified, or protected as 'Law Enforcement Sensitive' and therefore limited in its availability to seaport security directors.

Interviews with representatives of participating ports indicate that their most recent FS 311.12 compliance audits were conducted against the standards specified in the 2001 Port Security Standards Compliance Plan.

This means that they may be unaware of the changes in the security standards and practices in FS 311.12 (2009), and may not have undergone an FDLE-conducted audit against the revised statute.¹⁰

MTSA standards are performance-based and implemented according to identified risk. The USCG allows ports to modify and implement physical, personnel, and operational security measures to address the threat and risk profiles *specific* to their port and tenant operations.¹¹ USCG MTSA compliance audits are conducted against an approved Facility Security Plan (FSP), which includes a threat assessment specific to each port and not against prescribed standards, as is the case of FS 311 compliance audits. The USCG also issues instructional Navigational Vessel Inspection Circulars (NVICs), to provide guidance on federal compliance requirements.

Data Collection & Analyses

In order to better illustrate the challenges in aligning the standards and requirements of the state and federal statutes, both statutes are compared in a simple matrix contained herein. The matrix compares elements of the 2009 and 2001 FS 311.12 standards against those found in MTSA, 33 CFR Part 105 and NVIC 03-03, Change 2.

In addition, interviews were conducted with Florida's ports to identify and document specific issues and concerns relative to the dual security requirements. The ports were consistent in their call for coordination and, where possible, alignment of the state standards with the federal standards, especially in the creation of performance-based compliance requirements. Details of specific areas of overlap, redundancy, potential

¹⁰ One port indicated that an FDLE audit for compliance was conducted of their facility and operations subsequent to the 1 July effective date for the revised FS 311.12 (2009). However, the subject port's Director of Security indicated that he did not receive a written copy of the new security objectives and standards against which the port was evaluated until after the audit was conducted. Most of the ports interviewed indicated that they have still not received guidance or assistance from FDLE regarding their expectations for compliance with the significant changes included in FS 311.12 (2009).

¹¹ As previously noted, seaports do not have consistent access to meaningful transnational, national, regional, and local threat intelligence.

conflict, and inefficiencies are identified in the Comparative Analysis section of this report.

2.2 Comparison Matrix

Florida has led the nation in the development and implementation of seaport security standards to protect its commercial seaports and their operations from criminal and terrorist activities. FS 311.12 required the Office of Drug Control (ODC) in consultation with the Florida Seaport Transportation and Economic Development (FSTED) Council, and in conjunction with the Florida Department of Law Enforcement (FDLE) to develop a statewide security plan based upon the Florida Seaport Security Assessment 2000, otherwise known as the *Camber Report*. This plan was required to establish statewide minimum standards for seaport security, including “the prevention of criminal activity. ODC subsequently delivered the *Port Security Standards – Compliance Plan*, which contains the statewide minimum seaport security standards and identifies specific requirements that are included but are not limited to: access control and ID badges; visitor access; access gates; parking; fencing; lighting; signage; and, law enforcement presence, as mandated for compliance with FS 311.12.¹²

FS 311.12 (2009) does not include any changes to these minimum standards. However, the new *Seaport Security Inspection Methodology* includes:

- *Port Security Standards – Compliance Plan (2001)*;
- *FDLE Seaport Security Data Collection Uniform Guidelines for Field Inspection Activity*;
- Special Agent in Charge notes; and
- In-brief/out-brief guidelines.

The FDLE Seaport Security Data Collection Uniform Guidelines for Field Inspection Activity is modified as needed to address changes in Florida Statute 311, and/or changes in the security standards as recommended by the Standards Committee to the Legislature. FDLE is responsible for inspecting Florida’s 12 active public seaports identified in FS 311.09 against the reference standards and security objectives.

FS 311.12 was promulgated in the absence of any federal law relating to seaport security. Following the events of 9/11, the Maritime Transportation Security Act of 2002 (MTSA) was enacted to identify minimum security standards and performance objectives for U.S. commercial seaports, vessels, and operations. The U.S. Coast Guard adopted regulations to guide implementation of the provisions of MTSA. Subsequent to the nation-wide implementation of MTSA, Florida became

¹² The new Seaport Inspection Methodology consists of the Statewide Minimum Seaport Security Standards, FDLE Seaport Security Data Collection Uniform Guidelines for Field Inspection Activity, SAC notes and in/out brief guidelines.

the only state that required compliance with both state and federal regulations outlining security standards and practices applied to its commercial ports.

From left to right, the Comparison Matrix contained herein reflects the following:

- **Column A:** Identifies the statutory requirements for maritime security for application at identified Florida commercial seaports included in FS 311 (2009);
- **Column B:** Identifies the standards outlined in the *Port Security Standards Compliance Plan* released by ODC and FDLE in 2001;
- **Column C:** Identifies the standards for compliance with federal maritime security requirements mandated by MTSA, as directed in 33 CFR, part 105; and the U.S. Coast Guard's Navigation and Inspection Circular (NVIC) 03-03, Change 2;
- **Columns D, E & F:** Identifies the complementing requirements or industry "best practices" associated with CBP's programs for international trade and supply chain security; and
- **Column G:** Identifies the areas of overlap, redundancy, conflicts, or inefficiencies that exist between state and federal regulations related to each identified maritime security standard or security objective.

Page Left Blank Intentionally

| F.S. 311 (2009) | 311.09(311) | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|---|--|---|---|--|--|--|--|
| Security Standards - FS 311.12 (1) | | The statewide minimum security standards for seaport security applicable to seaports listed in FS 311.09 shall be based on the Florida Seaport Security Assessment 2000, and was set forth in the Port Security Standards Compliance Plan delivered to the Speaker of the House of Representatives and the President of the Senate on December 11, 2000. | Performance guideline standards for achieving compliance with MTSA requirements are outlined in 33 CFR Part 105 (Facilities), and U.S. Coast Guard Navigation and Inspection Circular (NVIC) 03-03, Change 2. The U.S. Coast Guard Sector Commander/Captain of the Port (COTP) has the authority to determine whether the preventive security measures adopted by the port achieve compliance with the regulation based on their ability to prevent or mitigate the credible threats and risks identified in the port's risk assessment. | C-TPAT recognizes that Marine Port Authority and Terminal Operators (MPTO) are already subject to defined security mandates created under the International Ship and Port Facility Security (ISPS) Code and the Maritime Transportation Security Act (MTSA). ISPS Code and MTSA compliance are a prerequisite for C-TPAT MPTO membership. | The Container Security Initiative (CSI) is a U.S. Bureau of Customs and Border Protection (CBP) program to increase security for container cargo shipped to the United States. The intent is to "extend the zone of security outward so that American borders are the last line of defense, not the first." CSI is implemented through the posting of U.S. Customs Service officers at foreign ports to work with their foreign counterparts to conduct screening of selected cargo containers | The Secure Freight Initiative is designed to help safeguard the global supply chain by evaluating cargo through scanning and data integration at selected overseas ports. As of Jan 26, 2009 CBP initiated a new rule titled "Importer Security Filing and Additional Carrier Requirements." This rule, known as the "10 + 2" Program, identifies the additional data elements required to be captured by the ocean carriers and importers to support the objectives of the SFI program. | Overlap: The intent of both federal and state and regulatory requirements is to create a secure operating environment for commerce at commercial ports. Conflict: FS 311.12 (2001) prescribed security standards are inflexible and conflict with the risk-based performance measures established by the USCG. Inefficiency: Compliance with the federal and state FS 311.12 (2001) requirements resulted in inefficient expenditure of funds for areas where compliance measures conflict. NOTE: FS 311.12 (2009) establishes requirement for closer alignment of state and federal seaport security standards and practices. In addition, waiver appeals are submitted to the Domestic Security Oversight Committee (DSOC) whose membership is overly represented by the State. In addition, the Seaport Security Standards Advisory Council has no role in the waiver appeal process. |
| 2. ID Badges - FS 311.12 | Security standards for ID badges are based on the Florida Seaport Security Assessment 2000, and set forth in the FDLE Port Security Standards Compliance Plan delivered to the Speaker of the House of Representatives and the President of the Senate on December 11, 2000. | a. All personnel permanently employed at the seaport (to include port management staff, tenant activity staff, truckers, stevedores, and longshoremen, etc.) will be required to display a picture ID badge or card at all times when accessing or working within areas as designated by port management. At a minimum, however, the following should be regarded as restricted areas: <ul style="list-style-type: none">• Cargo storage or staging yards• Docks/berths• Fuel storage or transfer yards• Cruise terminals This requirement also applies to day workers and casual labor that work at the port more frequently than 5 days in any given 90-day period. b. Picture IDs should be color coded or clearly identified by other means (e.g. hologram or symbol) to indicate areas to which access is authorized (e.g. docks, cargo yards, marine terminals, administration buildings, or unrestricted access). c. ID cards will be laminated and | The port's facility owner/operator must ensure that a TWIC program is implemented as follows: 1. All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access. 2. A TWIC is granted only after the successful completion of a criminal history background check by federal authorities. 3. The photo on the TWIC is compared against the presenting individual to confirm the identified of the TWIC holder. 4. Verification that the TWIC has not expired has been performed. 5. If an individual cannot present a TWIC because it has been lost or stolen, and he or she has previously been granted unescorted access to the facility and is known to have had a valid TWIC, the individual may be given unescorted access to secure areas for a period of no longer than 7 consecutive calendar days if the individual has reported that the TWIC | An employee identification system must be in place for positive identification and access control purposes. In accordance with foreign, federal, local, and state laws, background checks and investigations must be conducted for prospective employees as appropriate. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employees position. Application information, such as employment history and references must be verified prior to employment. Visitors, vendors government officials, and service providers must present photo identification for documented purposes upon arrival at the MPTO facility, and a visitor log must be maintained. Identification must be checked to ensure that it is a valid government-issued identification | CSI Not Applicable at US Ports. All CSI ports must comply with ISPS Code requirements. The ISPS Code recognizes MTSA compliant FSPs as meeting ISPS Code requirements. | Not Directly Applicable. Ocean carriers calling at U.S. ports must comply with MTSA requirements, which include the execution of a Declaration of Security that identifies the acceptable policies, procedures, and documentation for the ship's crew leaving and entering the port's restricted areas while their vessel is in port. | Conflict: State and federal seaport security ID and access control credentials conflict. Redundancy: Separate criminal background inspections for state and federal port ID and access control credentials are costly, and the source of a great deal of customer dissatisfaction. Conflict: FS 311.12 (2001) prescribed security standards are inflexible and conflict with the risk-based performance measures established by the USCG. Overlap: Disqualification criteria for issuance of an ID/Access Control credential are not necessarily consistent between federal and state criminal background investigations. |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | G-TPAT | GSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|-----------------|------------|--|--|--|-----|-----|---|
| | | <p>issued by serial number. Lost or stolen cards must be reported and a log maintained of all currently issued and restricted cards. (Continued below)</p> | <p>is lost or stolen to TSA as required by 49 CFR 1572.21.</p> <p>6. The individual can present another identification credential that meets the requirements of Section 101.515 of 33 CFR, Part 105.</p> <p>7. There are no suspicious circumstances associated with the individual's claim or loss or theft.</p> | <p>card that is not expired. Visitors, vendors, and service providers must also state where they are proceeding within the port to conduct business. Once fully implemented, the provisions of the Transportation Workers Identity Credential (TWIC) will serve to satisfy the criteria for renewal or denial of the required ID card.</p> | | | |
| | | <p>d. Issuance of the picture ID card by Port Management will be contingent on the successful completion of a fingerprint-based criminal history background check. The fingerprint-based criminal history shall be performed on any applicant for employment, every current employee, and other persons as designated pursuant to the seaport security plan. The criminal history check shall be performed in connection with employment within seaport property (including tenant areas) or other authorized regular access to a restricted access area, or the entire seaport if the seaport security plan does not designate one or more restricted access areas. With respect to employees or others with regular access, such checks shall be performed at least once every 5 years. The costs of the checks, consists with s. 943.053(3), shall be paid by the seaport or other employing entity or by the person checked. Policies, procedures, and criteria for the implementation of the fingerprint-based criminal history checks shall be included in the seaport security plan.</p> <p>e. Each seaport security plan shall identify criminal convictions or other criminal history factors which shall disqualify a person from either initial seaport employment or new authorization for regular access to seaport property or to a restricted access area. Such factors shall be used to disqualify all applicants for employment or others seeking regular access to the seaport or restricted area on or after January 2002 and may be used to disqualify all those employed or authorized for regular access on that date. In addition to other requirements for employment or access established by each seaport pursuant to its seaport security plan, each seaport plan shall provide that:</p> <ol style="list-style-type: none"> any person who has within the past 5 years been convicted, regardless of whether adjudication was withheld, for dealing in stolen property; any violation of s. 893.135; any violation involving the sale, manufacturing, delivery, or possession with intent to sell, manufacture, or deliver a controlled substance; burglary; robbery; any violation of s. 790.07; any crime of which includes use or possession of a firearm; any conviction for any similar offenses under the laws of another jurisdiction; or conviction for conspiracy to commit any of the listed offenses shall not be qualified for initial employment within or regular access to a seaport or restricted access area; and Any person who has at any time been convicted for any of the listed offenses shall not be qualified for initial employment within or authorized regular access to a seaport or restricted access area unless, after release from incarceration and any supervision imposed as a sentence, the person remained free from a subsequent conviction, regardless of whether adjudication was withheld, for any of the listed offenses for a period of at least 5 years prior to the employment or access date under consideration. <p>3. By October 1 of each year, each seaport shall report to the Department of Law Enforcement each determination of denial of employment or access and any determination to authorize employment or access after an appeal of a denial made during the previous 12 months. The report shall include the identity of the individual affected, the factors supporting the determination, any special condition imposed, and any other material factors used in making the determination.</p> <p>4. Policy, procedures, and criteria for the denial of employment or access to restricted areas based on criminal history factors shall be included in the seaport security plan.</p> <p>f. Each seaport security plan may establish a procedure to appeal a denial of employment of access based upon criminal history factors established per s. 311.12 (see Standard 1e.), the appeal procedure may allow the granting of waivers or conditional employment or access. In addition, a seaport may allow waivers on a temporary basis to meet special or emergency needs of the seaport or its users. Policies, procedures, and criteria for implementation of the appeals process shall be included in the seaport security plan.</p> <p>g. Port management must determine local procedures for permitting access by transient laborers or itinerant visitors and business people. At a minimum, these procedures will include logging in all personnel to whom a Port ID card has not been issued and issuance of a temporary or visitors pass.</p> <p>h. ID cards will be renewed on an annual basis. Any felony conviction for the crimes noted above during the previous year would constitute grounds for denial or disapproval.</p> | | | | | |

| F.S. 311 (2009) 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|--|---|---|---|--|--|---|
| 3. Personnel Security - FS 311.12 (7)(c) | <p>The seaport shall allow only individuals that can meet a high level security background check regular access to secure or restricted areas of the port and shall reduce seaport threats by allowing only such trusted individuals unescorted access into secure or restricted areas. A fingerprint-based criminal history check must be performed on all employee applicants, current employees, and other persons authorized to regularly enter a secure or restricted area, or the entire seaport if the seaport security plan does not designate one or more secure or restricted areas. Each individual who is subject to a criminal history check shall file a complete set of fingerprints taken in a manner acceptable to the Department of Law Enforcement for state processing. The results of the criminal history check must be reported to the requesting seaport and may be shared among seaports. All fingerprints submitted to the Department of Law Enforcement shall be retained.</p> | <p>Prospective employees will be required to provide background information about previous employment history, criminal records, and drug use. Prospective employees will also be fingerprinted as part of the application process.</p> | <p>MTSA requires that the Facility Security Plan (FSP) includes procedures for implementation of TWIC application, vetting, and issuance process. The TWIC process includes the requirement for conduct of a fingerprint-based background check of federal databases to determine whether the applicant has a history of any disqualifying factors in his background.</p> | <p>Once fully implemented, the provisions of the Transportation Workers Identity Credential (TWIC) will serve to satisfy the criteria of conducting background checks of U.S. MPTO Employees. MPTOs must have a written and verifiable procedures for the screening of service providers contracted to provide services within the confines of the port or terminal. MPTO must also have screening procedures for new customers, beyond financial soundness issues to include indicators of whether the customer appears to be a legitimate business or a security risk.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Conflict: Disqualification criteria associated with state and federal criminal background investigations are not the same. NOTE: FS 311.12 (2009) mandates alignment of state and federal criteria for criminal background investigations. Federal legislation is currently being considered that will prohibit the state from conducting additional criminal background checks on applicants for a state port access ID badge who have successfully had a federal background investigation completed and been awarded a TWIC.</p> |
| 4. Visitor Access | <p>a. Access to the seaport should require checking and recording the visitor's name, purpose of visit, destination, vehicle tag number, and date and time of entry/departure. b. Visitors should be authorized access only to area specific to their port business. Passes should be used to convey this permit. c. Visitors should not be allowed on the dock or in restricted areas and all vehicles must park in designated areas.</p> | <p>Newly-hired facility employees may be granted access to secure areas of the facility for up to 30 consecutive calendar days prior to receiving their TWIC provided all of the requirements are met, and providing that the new hire is accompanied by an individual with a TWIC while within the facility's secure area(s). The FSP must include procedures for preventing unescorted access to an area of the facility that is designed as a secure area unless the accessing individual holds a TWIC and is authorized to be in the area. Anyone that cannot present his or her TWIC for any other reason than those identified in the regulation may not be granted unescorted access to the secure area, and must be under escort at all times when inside the secure area</p> | <p>Visitors, vendors, government officials, and service providers must present photo identification for documentation purposes upon arrival at MPTOs facility, and a visitor log must be maintained. Identification must be checked to ensure that it is valid. Visitors, vendors and service providers should also state where they are proceeding to within the port to conduct business.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Directly Applicable. Ocean carriers calling at U.S. ports must comply with MTSA requirements, which include the Declaration of Security (DoS) that identifies the acceptable policies, procedures, and documentation to the visiting vessels while they are in port. Under MTSA, visitor access procedures for vessels while in port must be included in both the Facility Security Plan, and the DoS which is executed between the port and the visiting vessel.</p> | <p>Conflict: Different state and federal background investigation disqualification standards results in conflicts in the ports determining visitor compliance with state requirements when seeking access to the port based on the possession of a TWIC. NOTE: Recent alignments efforts of state and federal standards for conducting background checks are not yet to the point that they will eliminate the conflict. AERS still contains additional disqualifying factors not contained in the TWIC.</p> |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|--|------------|--|---|--|---|----------------|---|
| 5. Access Gates & Gate Houses - FS 311.12 | | <p>a. Gates and gatehouses should control access to restricted areas as determined by Port Management. Gates should be located at all perimeter access points and principal interior access points;</p> <p>b. Gates should be the minimum number to provide adequate access. c. Gates/gate houses should be staffed or locked at all times; d. The construction of the gates should at least match the construction on the perimeter or interior fencing in general. (e.g., 8 feet high, 9 gauge galvanized steel, of 2 inch wide chain link construction topped with an additional 2 foot barbed wire outrigger consisting of 3 strands of 9 gauge galvanized steel barbed wire at a 45 degree outward angle above the fence; e. Gatehouses at all vehicle entrances and exits should be staffed during business hours unless controlled by electronic access systems. Gatehouses should be situated so that exiting vehicles may be halted and examined on seaport property;</p> <p>f. Gatehouse personnel should be thoroughly trained in the procedures for processing and/or logging vehicular entry/exit; g. Gatehouse personnel should be equipped with telephones or other communications devices.</p> | <p>33 CFR Part 105 & NVIC 03-03, Change 2 requires each port to define the extent of their secure and restricted areas, and to establish points for controlling vehicle and personnel access into those areas. Under federal regulations these access gates and gatehouses must:</p> <ol style="list-style-type: none"> 1. Be manned by personnel with appropriate training in the port's policies and procedures for controlling vehicle and personnel access into the port's secure and restricted areas; 2. Be equipped with security systems or equipment to remotely control access of vehicles and personnel access into the facility's secure or restricted areas; 3. Have the capability for communicating changes in the threat profile or MARSEC levels that result in the changes in the manning or operations at the access gates and gate houses; 4. Be able to control the entry, parking, loading, and unloading of vehicles | Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored and secured when not in use. | CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements | Not Applicable | Conflict: FS 311.12 requires the presence of law enforcement officers at all vehicle and personnel entry gates into port restricted areas, while federal regulations allows for monitoring of gates and access control through technical means. |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|-----------------------------------|---|--|---|---|---|----------------|--|
| 6. Designated Parking - FS 311.12 | Subject to compliance with standards outlined in the 2001 Port Security Standards Compliance Plan, unless superseded by the award of an equivalency waiver or area exemption via the process established in FS 311.12 (2009). | a. Parking within the seaport should be severely restricted, and should be authorized by a strictly enforced gate pass and / or decal system. b. Passes or decals should be color or otherwise coded to further restrict access to authorized times and locations. c. Parking for employees, dock workers, and visitors should be restricted to designated areas, off dock and outside of fenced operational, cargo handling, and designated storage areas. d. Parking for vehicles authorized on port grounds should be restricted largely to port authority, carrier maintenance, commercial and government vehicles which are essential within the seaport or marine terminal. Parking for these vehicles should be restricted to fenced or clearly marked designated parking areas within the perimeter of the port. e. Temporary permits or passes should be issued to vendors and visitors for parking in designated controlled areas. | | Access to terminal by private passenger vehicles should be limited as much as possible in order to lessen opportunities to introduce contraband into the terminal area or to remove items from the terminal. If access is given to private vehicles they should be prohibited from parking in or adjacent to cargo handling and storage areas and vessels. Trucks with cabs/condos should be locked at all times while left unattended in the port to prevent absconders or stowaways from hiding in the conveyance to gain access outside of the port. | CSI Not Applicable at US Ports NOTE: All CSI ports must comply with ISPS Code requirements | Not Applicable | Inefficiency: FS-311.12 requirement for implementation of a vehicle decal program is viewed as inefficient, time consuming, and a waste of manpower and financial resources. Since there is no mechanism for enforcing this requirement or penalizing the ports for non-implementation the ports may choose non-compliance. Ports believe that vetting individuals at the ports access point is sufficient to protect the ports. Vetting vehicles is not a sensible expenditure of limited manpower and resources. |
| 7. Fencing - FS 311.12 | Subject to compliance with standards outlined in the 2001 Port Security Standards Compliance Plan, unless superseded by the award of an equivalency waiver or area exemption via the process established in FS 311.12 (2009). | a. Fencing should establish a secure perimeter with controlled access. b. Fencing should be 8 feet high, 9 gauge galvanized steel, of 2 inch wide chain link construction topped with additional 2 foot barbed wire outrigger consisting 3 strands of 9 gauge galvanized barbed wire at a 45 degree outward angle above the fence. c. Bottom of fencing should be no more than 2 inches from hard surface of concrete or asphalt. This surface should be sufficiently thick to prevent access from underneath. d. The exterior and interior sides of the fence should be cleared and uncluttered by not less than 5 feet to ensure the integrity of the fence is not compromised. e. (ADDITIONAL REQ FOR HI RISK PORTS) Reinforcement of the fence line with a barrier (e.g. ditch or berm) is recommended to enclose wheeled operations involving containers on chassis or truck loaded with consolidated cargo overnight. | MTSA requires the FSP to identify the boundary of the ports secure and restricted areas, and that fencing and barriers to protect the port's secure and restricted areas from access by unauthorized personnel and vehicles be in place. Fencing and barriers should be sufficient to deter unauthorized access into the port's secure or restricted areas commensurate with the threats and risks identified in the port's facility security plan. | Perimeter fencing should enclose the entire port area, and areas around cargo handling and storage facilities, container yards, and terminals. All fencing must be regularly inspected for integrity and damage. | CSI Not Applicable at US Ports NOTE: All CSI ports must comply with ISPS Code requirements | Not Applicable | Inefficiency: Implementing FS-311.12 standards for fencing results in expenditure of limited financial resources to secure an area to a degree that is inconsistent with the value of the material protected, or the category or degree of threat identified in the periodic risk assessments conducted of the port. NOTE: FS-311.12 (2009) creates a mechanism for the ports to request and receive area exemptions, or equivalency waivers from the minimum security standards for fencing identified in the Minimum Security Standards Compliance Plan. However, waiver appeals are presented to the Domestic Oversight Committee whose membership is heavily weighted toward State representatives. |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|-------------------------|------------|--|--|--|--|-----------------------|--|
| 8. Lighting - FS 311.12 | | <p>a. Lighting should be sufficient to adequately illuminate port operations and cargo areas. Port facilities should be illuminated at least to the level of twilight. Lighting must conform to federal regulations, and should comply with voluntary agreements such as the U.S. Customs Sea Carrier or Super Carrier Initiatives. b. Lighting must be provided sunset to sunrise. c. Lighting should be high-mast, sufficient for adequately illuminating exterior gates, piers, cargo areas, cargo traffic areas, and all working and walking areas. d. Updated lighting technology should be used, such as high pressure sodium, mercury vapor, or metal halide lighting. e. Lighting should be directed downward, away from guards or offices, and should produce high contrast with few shadows. f. Dock work areas, including container unloading and loading areas, should have 5 foot candle illumination. g. Container / cargo yards should have at least 1 foot candle illumination. Dark or blind spots should not exist. h. If security vehicles are used, they should be equipped with spotlights.</p> | <p>The Facility Security Assessment (FSA) Report must include a description of existing security measures, including lighting, for the facility and its secure or restricted areas. Lighting and illumination sufficient to facilitate monitoring of vehicles, personnel, and operations within the port's secure and restricted areas is required. Lighting should be augmented to facilitate monitoring access and movement adjacent to vessels and, where appropriate, use lighting provided by the vessel itself. Federal regulations seek to limit lighting effects, such as glare, that may have a negative effect on safety, navigation, or other security activities. Enhancements to protective lighting and illumination requirements associated with changes in the MARSEC level must be included in the FSP.</p> | <p>Adequate lighting must be provided inside and outside the facility, including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas. While at port, the pier and waterside of the vessels must be adequately illuminated.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable</p> | <p>Inefficiency: Implementing FS-311.12 standards for lighting results in increased expenditures of limited financial resources to illuminate an area to a degree that is inconsistent with the value of the material protected, or the category or degree of threat identified in the periodic risk assessments conducted of the port.</p> <p>Conflict: Implementing FS-311.12 standards for lighting are sometimes in conflict with local statutes or light pollution ordinances.</p> <p>Note: FS-311.12 (2009) creates a mechanism for the ports to request and receive area exemptions, or equivalency waivers from the minimum security standards for lighting and illumination identified in the Minimum Security Standards Compliance Plan. However, waiver appeals are presented to the Domestic Oversight Committee whose membership is heavily weighted toward State representatives.</p> |

| F.S. 311 (2009) 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap/Redundancy/Conflicts/Inefficiencies |
|--|---|---|--|--|--|--|
| <p>9. Use of Signs - FS 311.12 (C)</p> <p>Each seaport listed in s. 311.09 must clearly designate in seaport security plans, and clearly identify with appropriate signs and markers on the premises of a seaport, all secure and restricted areas as defined by the United States Department of Homeland Security-United States Coast Guard Navigation and Vessel Inspection Circular No. 03-07 and 49 C.F.R. part 1572.</p> <p>The seaport must provide clear notice of the prohibition against possession of concealed weapons and other contraband material on the premises of the seaport.</p> | <p>a. Signs should be strategically posted throughout the port and wherever access is restricted to authorized personnel. b. A sign conveying Customs authority and stating something similar to "This Port is a Border Entry Point and All Persons, Effects, and Vehicles are Subject to Search Under Federal Statute 19 U.S. Code Sec. 981(F)", should be posted at main exterior access points, vessel gangways, and all restricted areas. c. Signs should conform to these minimum standards and be highly visible with high contrast background and lettering. Signs should be visible at night, illuminated by lights or indelible lettering and be of sufficient size and boldness. Signs should be bilingual where appropriate.</p> | <p>MTSA requires that signs have been conspicuously posted describing the security measures in effect, and that states: 1. Entering the facility is deemed valid consent to screening or inspection. 2. Failure or refusal to consent or submit to screening or inspection will result in denial or revocation of authorization to enter the secured or restricted areas.</p> | <p>Compliance with MTSA requirements for this security measure is a prerequisite for MPTO C-TPAT membership.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable</p> | <p>Overlap: Requirements for signage are fairly consistent for state and federal standards. Signage language may vary from port to port.</p> |
| <p>10. Locks & Keys - FS 311.12</p> <p>Subject to compliance with standards outlined in the 2001 Port Security Standards Compliance Plan, unless superseded by the award of an equivalency waiver or area exemption via the process established in FS 311.12 (2009).</p> | <p>a. Key control should be implemented to delineate which personnel have right of access to specific areas. Key control should include a master ledger recording the legitimate holder of each copy of each key, issuance for which should be controlled by management or security personnel. b. Locks, locking devices, and key control systems should be inspected regularly and malfunctioning equipment repaired or replaced. c. Keys will be removed and secured from cargo handling equipment and vehicles when not in use. d. Only case hardened locks and chains will be used, with chains permanently attached to fence posts/gates.</p> | <p>Appropriate policies, procedures and practices for implementing measures for controlling locks, locking devices, and key control systems must be included in the FSP. The locks and locking devices used must be sufficient to provide an appropriate level of protection to the facility's areas, operations, and personnel being protected, based on the evaluation of the threat and risk identified in the port's facility security assessment. Key control policies and procedures are subject to inspection as part of the annual USCG compliance audit.</p> | <p>All external and internal windows, gates, and fences must be secured with locking devices. Management and security personnel must control the issuance of all locks and keys.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable to Florida's ports</p> | <p>Overlap: Requirements for implementation of key control measures are fairly consistent for state and federal standards. Federal standards may be adjusted by the COTP based on the credible threats and risks associated with the port, as determined by recurring port security assessments.</p> |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|---|------------|--|--|---|---|-----------------------------------|--|
| 11. Maintenance - FS 311.12 | | Subject to compliance with standards outlined in the 2001 Port Security Standards Compliance Plan, unless superseded by the award of an equivalency waiver or area exemption via the process established in FS 311.12 (2009). | <p>The FSP must include procedures to ensure that security systems and equipment are in good working order and are inspected, tested, calibrated, and maintained according to manufacturer's recommendations.</p> <p>The FSP must include procedures to ensure that security systems are regularly tested in accordance with the manufacturer's recommendations, that deficiencies noted are corrected promptly, and that the results are recorded as required. The FSP must also include procedures for identifying and responding to security system and equipment failures or malfunctions.</p> | Compliance with MTSA requirements for this security measure is a prerequisite for MPTO C-TPAT membership. | CSI Not Applicable at US Ports NOTE: All CSI ports must comply with ISPS Code requirements | Not Applicable | Overlap: Requirements for maintaining port security infrastructure, systems, and equipment is consistent between state and federal requirements. |
| 12. Standing Security Committee - FS 311.12 | | <p>Florida Legislative Standard B1</p> <p>Has port management created a standing security committee, and is a forum conducted at least once per quarter to which all stakeholders in port security are invited to discuss security measures?</p> | <p>MTSA established Area Maritime Security Committees under the control of the U.S. Coast Guard's Sector Commander, which is used to coordinate security policies, and incident notification response, and recovery procedures included in the Area Maritime Security Plan.</p> <p>Participation in the AMSP is a required for each port that is subject to 33 CFR part 101 each port is required to participate in the AMSP.</p> | Compliance with MTSA requirements for participation in the Area Maritime Security Committee is a prerequisite for MPTO C-TPAT membership. | CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements | Not Applicable to Florida's ports | Overlap: Both state and federal regulations call for port security management participation in forums where security is discussed. FS 311.12 mandated port security committees are limited to the port operator, tenants, and other appropriate local or municipal authorities. The federal statute established the Area Maritime Security Committee (AMSC) which encompasses a broader range of participants from the port, law enforcement, municipal government, and supporting infrastructure and supply chain management entities. These two entities are viewed as mutually supporting without unnecessary redundancy. |

| F.S. 311 (2009) 311.09/311 311.12 (3) (a) (b) | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|---|---|---|--|---|---|--|
| <p>13. Security Master Plan - FS</p> <p>FS 311.12(2)(b) Each seaport listed in 311.09 shall adopt and maintain a security plan specific to that seaport which provides for a secure seaport infrastructure that promotes the safety and security of state residents and visitors, and the flow of legitimate trade and travel. Each seaport security plan shall be approved by the Florida Department of Law Enforcement (FDLE), the Governor's Florida Office of Drug Control (ODC) and the United States Coast Guard (USCG): 1. Does the seaport have a security plan as adopted by the Florida Legislature Standard Date? 2. Has the security plan been reviewed and approved by FDLE after 1 Jan 2007? 3. Has the security plan been reviewed and approved by the Office of Drug Control? 4. Are there any plan amendments pending approval and have all such amendments been submitted to the USCG, FDLE, and ODC? 5. What is the date of last revision of the seaport security plan? 6. Is there evidence of participation and or assistance by the Regional Domestic Security Task Force (RDSTF) in the revision of the seaport security plan? 7. Is there evidence of participation by the USCG in conjunction with the port in revision of the seaport security plan? 8. Are security related initiatives included in the port's strategic or master plan? 9. Are capital projects for security initiatives included in the port's strategic or master plan?</p> | <p>a. Port Management will include security-related initiatives in the port's strategic or master plan. These initiatives should identify and prioritize projected capital outlays for security-related projects.</p> | <p>U.S. Coast Guard NVIC 03 03, Change 2 details Facility Security Plan implementation, the plan review process, provides guidance to successfully execute compliance inspections, adds information for guidance for the purposes of performing facility assessments, and provides clarification on the applicability of MTSA mandated regulations found in 33 CFR part 105. All facilities subject to 33 CFR 105 must submit Facility Security Plans to the cognizant Captain of the Port (COTP) in accordance with 33 CFR 105.310, 33 CFR 105.410 and, if applicable, HOMEPOR guidance. The FSP review process is critical to the successful implementation of MTSA regulations. An on-site verification may be necessary, depending on the familiarity of the plan reviewer with the specific facility. Facilities must comply with their security plan while conducting regulated operations or risk enforcement actions, which may include suspension of operations until compliance is reached. Major deficiencies noted during a FSP review will require the plan to be resubmitted with corrections prior to further review. Major deficiencies include: 1. An incomplete or missing Facility Vulnerability and Security Measures Summary (Form CG-6025). 2. An incomplete or missing Facility Security Assessment (FSA) report, and/or 3. Two or more incomplete FSP content requirements.</p> | <p>US and foreign-based MPTOs must conduct a comprehensive assessment of their security practices based on C-TPAT minimum-security criteria, and shall have a documented and verifiable process for security vulnerabilities within their operations based on their business model. C-TPAT recognizes that MPTOs are already subject to defined security mandates created under the ISPS Code and the MTSA. C-TPAT</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable to Florida's ports</p> | <p>Overlap: Both state and federal regulations call for the development of a port/facility security plan that includes an assessment of the threats and risks associated with the port and its operations, and includes the practices and procedures required to comply with the identified standards. Conflict: Formatting and content language requirements for state vs. federal security plan documents sometimes require duplicative sections or language to address requirements specific to either the state or federal standard being addressed. NOTE: FS 311.12 (2009) mandates alignment of state and federal standards and requirements. Lack of standardized language creates confusing conflicts or duplication in the facility security plan documentation.</p> |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|--|------------|---|--|---|--|--|---|
| 14. Standard Operating Procedures - FS 311.12 | | | | | | | |
| Florida Legislature Standard B 3 a Operational and procedural security must be sound to secure the port. Port management should, through formal adoption of security procedures, ensure that management sends a message that security is taken seriously at the port. Has port management provided a current security manual, including standards of conduct to appropriate management personnel? Has port management provided a current security manual including responsibilities to appropriate management personnel? Has the port security director formulated written operating procedures for bomb threats? Has the port security director formulated written operating procedures for alert levels? | | <p>a. Port Management shall provide a current security manual incorporating standard operating procedures, responsibilities of appropriate security and management personnel, and a definitive statement of what management expects of its security force personnel. b. Managers must review procedures periodically to ensure that new threats and procedural vulnerabilities are identified as they arise. c. The Port Security Director should formulate written operation procedures for security-related matters, including bomb threats and alert levels, and should collaborate with relevant government and law enforcement agencies to develop an emergency response plan.</p> | <p>MTSA requires the development of a Facility Security Plan (FSP) that identifies standard operating procedures for: 1. Determining who is authorized unescorted access into the port's secure and restricted areas. 2. Implementation of the procedures for controlling vehicle and personnel access into the port and its secure and restricted areas. 3. Responding to changes in the MARSEC levels, security threats or incidents. 4. Interfacing with vessels entering into the port at all MARSEC levels. 5. Determining which vehicles and personnel who have a valid reason for unescorted or escorted access into the port. 6. Restricting unescorted port access to vehicles and personnel who cannot demonstrate a valid need for access into the port's secure or restricted areas.</p> | <p>Compliance with MTSA requirements for the development, maintenance, and annual inspection of a USCG-approved Facility Security Plan (FSP) is a prerequisite for MPTO C-TPAT membership</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable to Florida's ports</p> | <p>NOTE: Alignment of state and federal standards addresses the reduction of formatting or language content conflicts in SOPs used to direct implementation of the FSP.</p> |
| 15. Law Enforcement Presence - FS 311.12/FS 311.122 | | | | | | | |
| Subject to compliance with standards outlined in the 2001 Port Security Standards Compliance Plan, unless superseded by the award of an equivalency waiver or area exemption via the process established in FS 311.12 (2009). | | <p>a. Port Management will take steps necessary to ensure the routine, scheduled presence at the port of security patrols by sworn law enforcement personnel. b. (ADDITIONAL REQ FOR HI RISK PORTS) Management should work with local authorities to negotiate for the permanent assignment to the port of a dedicated, full-time unit of sworn law enforcement.</p> | <p>Commercial seaports are border entry and control points into the United States. As a result, Federal law enforcement officers (e.g. Customs Inspection, Border Protection & Immigration Officers), are a normal presence at U.S. commercial seaports. Under MTSA their presence and abilities to respond to threats and changes in the MARSEC level are integrated into the Area Maritime Security Plan.</p> | <p>Compliance with MTSA requirements for the presence and participation of federal law enforcement officers is a prerequisite for MPTO C-TPAT membership.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable to Florida's ports</p> | <p>Conflict: FS 311.12 (2001) establishes a requirement for the use of state certified law enforcement officers to perform patrol functions at seaports. Depending on the size and nature of the port, a sizeable contingent of federally-certified law enforcement officers may be present at the port as well. These officers are not recognized as meeting the state requirement as their primary functions are not limited to the state-mandated patrol functions, and may conflict with emerging security response requirements on the port.</p> |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|--|------------|--|--|---|--|-----------------------|--|
| 16. Security Guards - FS 311.12/FS 311.121 | 311.09/311 | <p>a. Guard or security personnel should wear uniforms that are complete, distinct, and authoritative. b. Guards and security personnel should have 2-way radios with capability to promptly reach back-up support. c. Guards and security personnel should provide adequate patrols to include roving security, building, perimeter, and wharf checks. d. Guards and security personnel should control all exterior access points and principal interior access points to the seaport. e. Guards and security personnel should be sufficient in number to provide adequate security 24 hours a day. f. Guards and security personnel should be properly trained and be state certified class D license holders. Non-sworn security personnel working for a local law enforcement agency and assigned to the port do not require a class D license. Training of security force personnel should include the following:</p> <ol style="list-style-type: none"> 1. Patrol methods 2. Report writing, log and record keeping 3. ID of security problems and specific trouble areas 4. Cargo handling and cargo documentation handling 5. Federal security procedures (DOO 5225.22M) 6. U.S. Customs, Immigration and Naturalization Service, and U.S. Coast Guard requirements 7. State Guard requirements 8. State procedures (including Port Authority) 9. Local police procedures 10. Hazardous materials transport and hazardous materials response 11. First aid 12. Use of force and weapons 13. Explosives, nuclear, biological, chemical agent response 14. Terrorism response procedures 15. Labor unrest | <p>33 CFR 105.210 requires the following training for all facility personnel with security duties:</p> <ol style="list-style-type: none"> 1. Current security threats and patterns. 2. Recognition and detection of dangerous substances and devices. 3. Recognition of characteristics and behavioral patterns of persons who are likely to threaten security. 4. Techniques used to circumvent security systems. 5. Crowd management and control techniques. 6. Security-related communications, including handling of CSI. 7. Knowledge of emergency procedures and contingency plans. 8. Operations of security equipment and systems. 9. Testing, calibration, operation, and maintenance of security equipment and systems. 10. Inspection, control and monitoring techniques. 11. Relevant provisions of the Facility Security Plan (FSP). 12. Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores. 13. The meaning and consequential requirements of the differing MARSEC levels. 14. Familiarity with all relevant aspects of the TWIC program and how to carry them out. | <p>The MPTO should ensure that security guards are manning entry and exit gates, and should include roving patrols to monitor sensitive areas, and areas that handle and store cargo. MPTO security personnel should conduct routine liaison with government personnel assigned to the port and vessel security personnel. If a Facility Security Officer (FSO) has been designated per MTS/ISPS Code, the FSO should be the MPTO's point-of-contact for all C-TPAT matters relating to security.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable</p> | <p>NOTE: FS 311.12 establishes minimum standards for training and certification of contract security guards performing security duties at Florida's seaports. Conflict/Inefficiency: The state standards for training and certification of Class D or Class G guards serving on commercial seaports does not include the subjects required for training of personnel with specific security duties identified in the federal regulation.</p> |

| F.S. 311 (2009) 311.09/311 - FS 311.12/FS 311.13 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|--|---|--|---|--|-----------------------|---|
| <p>Seaport security plans created pursuant to 311.12 are exempt from FS 119.07(1). Article 1 of the State Constitution. In addition, photographs, maps, blueprints, drawings, and similar materials that depict critical seaport operating facilities are exempt from FS 119.07(1) and S2(a). Article 1 of the State Constitution, to the extent that a seaport reasonably determines that such items contain information that is not generally known and that could jeopardize the security of the seaport. However, information relating to real estate leases, layout plans, blueprints, or information relevant thereto is not included in this exemption.</p> | <p>a. Formal guidelines for computer security (INFOSEC) should be in place for each port and tenant activity.</p> <p>b. Computerized information access must be password controlled and should be restricted on a need-to-know basis, which would include dissemination of information no sooner than required.</p> | <p>Security assessments, security plans and their amendments contain information that, if released to the general public, would compromise the safety or security of the port and its users. This information is known as Sensitive Security Information (SSI), and the Transportation Security Administration (TSA) government the handling of SSI Materials through 49 CFR 1520, Protection of Sensitive Security Information. These regulations allow the Coast Guard to maintain national security by sharing unclassified information with various facility and vessel personnel without releasing SSI to the public. Facility owners and operators must follow procedures stated in 49 CFR 1520 for the marking, storing, distributing, and destroying of SSI materials, which includes many documents that discuss screening processes and detection procedures. Under these regulations only persons with a "need to know", as defined in 49 CFR 1520.11, will have access to security assessments, plans and amendments. Facility owners or operators must determine which of their employees have a need to know the provisions of the security plans and assessments, and restrict dissemination of these documents accordingly. To ensure that access is restricted only to authorized personnel, SSI material will not be disclosed under the Freedom of Information Act (FOIA) for most circumstances.</p> | <p>Automated systems must use individually assigned accounts that require a periodic change of password. IT security policies, procedures and standards must be in place and provided to employees in the form of training. A system must be in place to identify the abuse of IT, including improper access, tampering or the altering of business data. All system violators must be subject to appropriate disciplinary actions for abuse.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable</p> | <p>Not Applicable</p> |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C:TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|----------------------------------|------------|---|---|--|--|-----------------------|--|
| 18. Cargo Processing - FS 311.12 | | <p>Subject to compliance with standards outlined in the 2001 Port Security Standards Compliance Plan, unless superseded by the award of an equivalency waiver or area exemption via the process established in FS 311.12 (2009).</p> <p>a. Gate passes should be issued to truckers and other carriers to control and identify those vehicles authorized to pick up cargo.</p> <p>b. Cargo should only be released to the carrier specified in the delivery order unless a release authorizing delivery to another carrier is presented and verified.</p> <p>c. Personnel processing delivery orders should verify the identity of the trucker and truck company before allowing entrance to or exit from restricted areas.</p> | <p>The FSP must ensure that security measures relating to cargo handling are implemented in order to: 1. Deter tampering. 2. Prevent cargo that is not meant for carriage from being accepted and stored at the facility without the knowledge and consent of the facility owner or operator. 3. Identify cargo that is approved for loading onto vessels interfacing with the facility. 4. Include cargo control procedures at access points to the facility. 5. Identify cargo that is accepted for temporary storage in a restricted area while awaiting loading. 6. Restrict the entry of cargo to the facility that does not have a confirmed date for loading. 7. Ensure the release of cargo only to the carrier specified in the cargo documentation. 8. Coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedures. 9. Create, update, and maintain a continuous inventory, including location of all dangerous goods or hazardous substances from receipt to delivery within the facility, and identifying the location of those dangerous goods or hazardous substances. 10. Ensure that appropriate increased security measures are implemented in response to MARSEC level changes.</p> | <p>Cargo should be tallied at the time of delivery to the consignee or his agent. In the event of any discrepancies at the time of delivery a manifest discrepancy report must be completed and provided to CBP. Arriving cargo should be reconciled against information on the cargo manifest described, and the weights, labels, marks and piece count indicated and verified. Cargo should be verified against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before the cargo is received or released.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable</p> | <p>NOTE: Alignment of state and federal standards address the elimination or reduction of conflicts in the requirements for processing, handling and storage of cargo.</p> |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|---|------------|--|--|--|---|---|--|
| 19. Storage of Loose Cargo - FS 311.12 | | | | | | | |
| Subject to compliance with standards outlined in the 2001 Port Security Standards Compliance Plan, unless superseded by the award of an equivalency waiver or area exemption via the process established in FS 311.12 (2009). | | <p>a. Cargo stored in open areas, and palletized or stacked cargo stored in warehouse facilities, must be properly stacked and placed within, away from, and parallel to fences and walls, to ensure unimpeded views for security personnel.</p> | <p>The FSP must contain procedures to ensure the security of all vessel stores and bunkers, and to ensure that these security measures are implemented as outlined in the FSP. These procedures must include advance notification of vessel stores or bunker deliveries, including a list of stores, delivery vehicle driver and vehicle registration information. Screening rates for vehicles and stores at each MARSEC level.</p> | <p>Compliance with MTSA requirements for this security measure is a prerequisite for MPTO C-TPAT membership.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable to Florida's ports</p> | <p>NOTE: Alignment of state and federal standards address the elimination or reduction of conflicts in the requirements for processing, handling and storage of loose or certain dangerous cargo.</p> |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|----------------------------------|------------|---|--|--|--|--|---|
| 20. High Value Cargo - FS 311.12 | | <p>Subject to compliance with standards outlined in the 2001 Port Security Standards Compliance Plan, unless superseded by the award of an equivalency waiver or area exemption via the process established in FS 311.12 (2009).</p> <p>a. High value commodities should be stored in cribs or security cages designed to resist forcible entry from all sides, and separate logs and procedures for the release and receipt of these commodities should be maintained. b. High value merchandise in mounted containers must be placed in a secure holding area where it can be observed by management or security personnel, and separate logs and procedures for the release and receipt of these containers should be maintained. c. High value cargo containers requiring storage should be placed in a systematic manner such that their location is not readily apparent to would be criminals. Doors of high value containers should be stacked so that the doors of each container abut each other.</p> | <p>33 CFR Part 105.295 establishes the procedures for ensuring security measures for the handling of cargo as outlined in the FSP. These procedures include:</p> <ol style="list-style-type: none"> 1. Routine checking of cargo, cargo transport units, and cargo storage areas within the facility prior to and during cargo handling operations for evidence of tampering. 2. Checking that cargo, containers, or other cargo transport units entering the facility match the delivery note or equivalent cargo documentation. 3. Screen vehicles. 4. Check seals and other methods used to prevent tampering with cargo upon entering the facility and storage within the facility. 5. Additional cargo security monitoring and protection measures to be implemented at increased MARSEC levels. <p>3 CFR Part 105.295 identifies specific security measures required for Certain Dangerous Cargo (CDC) facilities:</p> <ol style="list-style-type: none"> 1. Escorting all visitors, contractors, vendors, and other non-facility employees. 2. Controlling parking, loading, and unloading of vehicles within a facility. 3. Requiring security personnel to record or report their presence at key points during security patrols. 4. Searching key areas prior to vessel arrivals. 5. Providing an alternate or independent power source for security and communications systems. | <p>The MPTO must store containers in their custody in a secure area to present unauthorized access and/or manipulation. Procedures must be in place for reporting detected, unauthorized entry into containers or container storage areas to appropriate local law enforcement officials. Containers should be segregated according to HAZMAT and temporary storage designations. MPTOs should institute practices to routinely check storage areas for cargo/containers. Empty containers should be checked to ensure that they are empty and devoid of false compartments.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable to Florida's ports</p> | <p>NOTE: Alignment of state and federal standards addresses the elimination or reduction of conflicts in the requirements for processing, handling and storage of high value cargo.</p> |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|-----------------------------------|------------|--|---|--|--|-----------------------|---|
| 21. Equipment Control - FS 311.12 | | <p>Subject to compliance with standards outlined in the 2001 Port Security Standards Compliance Plan, unless superseded by the award of an equivalency waiver or area exemption via the process established in FS 311.12 (2009).</p> <p>a. Access and keys to cargo handling equipment such as yard mule tug-masters, trucks, or high loaders should be strictly controlled. Cargo handling equipment should be kept in a secure and specified area when not in use.</p> | <p>Policies and procedures for controlling access to and security of security systems and equipment must be included in the FSP. The FSP must also include requirements for maintaining records relating to the periodic testing, maintenance, and replacement of security systems and equipment.</p> | <p>Compliance with MTSA requirements for this security measure is a prerequisite for MPTO C-TPAT membership.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable</p> | <p>Not Applicable</p> |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C:TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|--|------------|--|--|----------------|---|----------------|--|
| 22. Cruise Operations Security - FS 311.12 | | <p>Subject to compliance with standards outlined in the 2001 Port Security Standards Compliance Plan, unless superseded by the award of an equivalency waiver or area exemption via the process established in FS 311.12 (2009).</p> <p>a. Adhere to U.S. Coast Guard regulations 33 CFR Part 120 and 33 CFR Part 128. b. Port Management will provide SOPs, used at passenger terminals, to all security personnel. c. Port management will provide and maintain physical security barriers, alarms, and lighting in accordance with IMO 443. d. Ensure that vehicular access to cruise ships, while in port, is strictly enforced and that only authorized vendors are permitted access to cruise ships. e. Provide communications between all security personnel involved with the security of passenger terminal and vessels. f. Establish a system of identification and control for all personnel authorized access to the terminal. g. Designating restricted areas for the embarking and disembarking of both passengers and baggage. h. Ensure that carries provide timely, accurate, and complete passenger and crew arrival and departure manifest information (in accordance with the Advanced Passenger Information System) to the Immigration and Naturalization Service and the U.S. Customs Service. i. Restrict access to passenger terminal facilities and cruise ships through a designated screening point that includes a metal detector and x-ray system for carry-on items.</p> | <p>The FSP must identify, at all MARSEC Levels, the security measures that have been established in coordination with a vessel moored at the facility and:</p> <p>1. Establish separate areas for segregation of checked from unchecked persons and personal effects. 2. Denying passengers access to secure and restricted areas unless supervised by facility personnel. Providing sufficient security personnel to monitor all persons in a facility with a public access area. At MARSEC Level 2: the owner/operator of a passenger facility with a public access area must increase the intensity of monitoring of the public access area. At MARSEC Level 3: in addition to the MARSEC Level 1 & 2 requirements the owner/operator of a passenger facility must increase the intensity of monitoring, and assign additional security personnel to monitor the public access areas. At all MARSEC Levels the facility owner/operator, in coordination with a vessel moored at the facility, must ensure the following security measures: a. Screening of all persons, baggage, and personal effects for dangerous substances and devices. b. Checking the identification of all persons seeking to board the vessel. For persons not holding a TWIC this check includes confirming the reason for boarding by examining joining instructions, passenger tickets, boarding passes, government identification or visitor badges, or work orders. c. Designate holding, waiting, or embarkation areas within the facility's secure area to segregate screened persons and their personal effects from unscreened persons and their personal effects. d. Provide additional security personnel to designated holding, waiting, or embarkation areas within the facility's secure area. e. Denying individuals not holding a TWIC access to secure and restricted areas unless escorted.</p> | Not Applicable | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | Not Applicable | <p>Conflict: ID and access requirements for cruise terminal employees are not aligned between state and federal requirements to support the cost and operationally effective conduct of cruise operations.</p> |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C:TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|--|------------|--|--|---|--|-----------------------|---|
| 23. Intrusion Detection System - FS 311.12 | | <p>a. (ADDITIONAL REQ FOR HI RISK PORTS) Closed Circuit Television cameras should be used when warranted by security threat. Cameras should be placed at main entrances and exits and in areas with high risk and/or high value cargo.</p> <p>b. (ADDITIONAL REQ FOR HI RISK PORTS) Cameras should be able to record at relatively low levels of light.</p> <p>c. (ADDITIONAL REQ FOR HI RISK PORTS) Cameras should have a remote control and zoom lens capability when used for surveillance.</p> <p>d. (ADDITIONAL REQ FOR HI RISK PORTS) Cameras should have video tape recording capabilities and be capable of being monitored at same time.</p> <p>e. (ADDITIONAL REQ FOR HI RISK PORTS) Cameras should be positioned, with a recording mechanism, to video record vehicles and pedestrians entering and exiting the facility.</p> | <p>The FSP must include a description of security measures that have the capability to continuously monitor, through a combination of lighting, security guards, waterborne patrols, automatic intrusion-detection devices, surveillance equipment, or any other security measures for each of the following facility features.</p> <p>1. Facility and its nearby land and waterside approaches. 2. Restricted areas within the facility. 3. Vessels at the facility and/or areas surrounding the vessels.</p> <p>At MARSEC level 1 the approved FSP must ensure that the security measures are implemented at all times, including the period from sunset to sunrise and periods of limited visibility. For each facility the FSP should ensure monitoring capabilities as follows:</p> <p>1. When automatic intrusion detection devices are used an audible or visual alarm is activated that is either continuously attended or monitored. 2. Provisions for monitoring equipment to function continually, including considerations of possible effects of weather or power disruptions. 3. Monitors the facility area, including shore and waterside access. 4. The capability to monitor access points, barriers, and restricted areas. 5. The capability of monitoring access and movements adjacent to vessels using the facility, including augmentation of lighting provided by the vessel itself. 6. Provisions to limit lighting effects, such as glare, and their impact on safety, navigation, and other security activities.</p> | <p>Alarm systems and video surveillance cameras should be utilized to monitor the premises and prevent unauthorized access to the port, terminal facilities, vessels, cargo handling and storage areas at those locations determined appropriate by the facility's risk assessment.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable</p> | |

| F.S. 311 (2009) 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|---|---|--|--|--|----------------|--|
| 24. Conduct of Ongoing Risk Assessments (ORA) - FS 311.12 | FS 311.12(1) Each seaport will continuously examine threats through a coordinated mechanism involving regional partners and update security plans as appropriate, commencing July 1, 2009 each port will develop and maintain a Director's Ongoing Risk Assessment (ORA). The seaport director will revise the seaport security plan as necessary based on the findings of the ORA. The ORA will be indicative of the analysis of general crime, cargo theft, internal conspiracy drug smuggling, acts of terrorism, and emerging trends of criminal activity that may affect the seaport. The observations, findings, and conclusions in the ORA will be incorporated into the procedures and mitigation strategies outlined into the Facility Security Plan to ensure that the seaport is in substantial compliance with the statewide minimum standards established pursuant to FS 311.12(1). | 33 CFR Part 105.305; 105.305(3); 105.305 1.1: 1. Has an on scene Facility Security Assessment been conducted and is there a written summary in the files of the port? 2. Does the Facility Security Assessment that has been conducted accurately reflect the description of existing security measures, including inspection control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control and similar systems? 3. Do the vulnerabilities in the FSA compare to the vulnerabilities in the quarterly threat and harm to human life assessments required in Florida law? 4. Do the following elements in the FSA compare to the ORA and is the FSA complete. 5. Is there a list of persons, activities, services and operations that are important to protect each of the categories within the FSA and does it compare to the ORA required in Florida law. | C-TPAT recognizes the complexity of marine port and terminal operations and enforces the application and implementation of security measures based upon risk. MPTOs shall have a documented and verifiable process for assessing the vulnerabilities within their operations based on their business model (i.e. volume, country of origin of incoming vessels and cargo, foreign ports identified by US Coast Guard as having inadequate security routing of incoming vessels/cargo, security alerts via open source information, phase security incidents, etc.) | CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements | Not Applicable | Overlap: State and federal requirements for seaport threat and risk assessments are not aligned to prevent unnecessary duplication of effort and unnecessary expenditure of resources. |
| | <p>Not Applicable - Not addressed in FS 311.12 (2001)</p> <p>1. Does the seaport's ORA include general crime, cargo theft, internal conspiracy, drug smuggling and terrorism information and analysis sufficient for the purpose of modifying the port security plan if necessary? 2. Is there evidence that the seaport periodically reviews and updates the security procedures, planning, and mitigation strategies relative to the observations and findings of the ORA?</p> <p>3. Is there evidence that security concerns and observations identified by the Seaport Standing Security Committee are incorporated into the ORA? Is there evidence that the seaport has modified the FSP based on threats identified in the ORA?</p> <p>Every 5 years after January 1, 2007 each seaport director, with the assistance of the Regional Domestic Security Task force and in conjunction with the United States Coast Guard, shall revise the seaport's security plan based on the director's ongoing assessment of security risks, the risks of terrorist activities, and the specific and identifiable needs of the seaport for ensuring that the seaport is in substantial compliance with minimum security standards established under subsection (1).</p> | <p>6. Does the FSA report account for vulnerabilities in the identified areas and do they compare to the ORA required in Florida law.</p> <p>7. Does the FSA report discussion and evaluation of procedures identified to evaluate the performance of security duties compare to the ORA required in Florida law?</p> <p>8. Does the FSA report include discussion and evaluation of procedures identified for controlling access to the facility through the use of identification systems, or otherwise compare to the ORA?</p> <p>9. Does the FSA report include discussion and evaluation of procedures identified for controlling the embarkation of vessel personnel and other persons and their effects, including personal effects and baggage whether accompanied or unaccompanied compare to the ORA?</p> <p>10. Does the FSA report include discussion and evaluation of procedures for handling of cargo and the delivery of vessel stores compared to the ORA?</p> <p>11. Does the FSA report include discussion and evaluation of procedures for the monitoring of restricted areas to ensure that only authorized persons have access compare to the ORA?</p> <p>12. Does the FSA report include discussion and evaluation indicating that there is readily available security communications, information and equipment, and does it compare to the ORA?</p> <p>13. Do the descriptions of the vulnerabilities with the FSA report correlate with the vulnerabilities identified within form CG-6025, the ORA, and the approved security plan?</p> <p>14. Do the descriptions of security measures found within the FSA report and the FSP correlate with the security measures identified within Form CG-6025, the ORA, and the approved security plan?</p> | | | | |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C:TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|---|------------|--|---|--|---|-----------------------|--|
| 25. Use of Alternative Security Standards - FS 311.12 (1)(b) FS 311.12 (8) To ensure an effective and efficient security apparatus, seaports may operate under alternative standards when such standards are threat based and approved. The seaport may be granted equivalency waivers that create alternate means of compliance from the standards when such alternate means do not diminish the safety or security of the seaport based on an extensive risk analysis by the seaport director. | | Not Applicable - Not addressed in FS 311.12 (2001) | 33 CFR part 105.140 provides for the submission of an Alternative Security Program (ASP) for acceptance by the USCG COTP. The USCG approved ASP used by the facility must have a letter signed by the facility owner or operator certifying that the facility is in full compliance with the measures outlined in the ASP. | Not Applicable - USCG Sector Commander has authority to waive requirements, or accept alternative security measures as appropriate to the threat, risk, and nature of the facility and its operations. | CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements | Not Applicable | Conflict: Lack of coordination to support alignment of alternative or equivalent security standards between state and federal requirements. |
| 26. Waiver from Security Requirements- FS 311.12(8) The Office of Drug Control and the Department of Law Enforcement may modify or waive any physical facility requirement or other requirement contained in the minimum security standards upon a determination that the purpose of the standards have been reasonably met or exceeded by the seaport requesting the modification or waiver. An alternate means of compliance must not diminish the safety or security of the seaport and must be verified through an extensive risk analysis conducted by the seaport director. | | Not Applicable - Not addressed in FS 311.12 (2001) | The USCG COTP has the authority to issue a letter for equivalency waivers to the security requirements identified in the FSP, as long as the alternative measures sufficiently address the threats and risks identified in the risk assessment associated with the facility, and do not diminish the level of security appropriate the value of the facility's operations and materials requiring protection. | Not Applicable - USCG Sector Commander has authority to waive requirements, or accept alternative security measures as appropriate to the threat, risk, and nature of the facility and its operations. | CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements | Not Applicable | Conflict/Inefficiency: State process for review and approval of waiver requirements is not as responsive as federal process. |

| F.S. 311 (2009) 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|---|--|---|--|--|----------------|--|
| 26. Possession of Valid TWIC - FS 311.12 | | | | | | |
| Any person seeking authorization for unescorted access to secure and restricted areas of a seaport must possess, unless waived under FS 311.12(7)(9e). FDLE shall establish a waiver process for an individual who does not have a TWIC, obtained a TRIC through a federal waiver process, or is found to be unqualified under FS 311.12 (7)(9a) and denied employment by a seaport or unescorted access to secure or restricted areas. If the seaport issues its own identification card in addition to the TWIC, that ID card must meet specific physical requirements. | Not Applicable - Not addressed in FS 311.12 (2001) | <p>The port's facility owner/operator must ensure that a TWIC program is implemented as follows:</p> <ol style="list-style-type: none">1. All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access.2. A TWIC is granted only after the successful completion of a criminal history background check by federal authorities.3. The photo on the TWIC is compared against the presenting individual to confirm the identified of the TWIC holder.4. Verification that the TWIC has not expired has been performed.5. If individuals cannot present a TWIC because it has been lost or stolen, and he or she has previously been granted unescorted access to the facility and is known to have had a valid TWIC, the individual may be given unescorted access to secure areas for a period of no longer than 7 consecutive calendar days if the individual has reported that the TWIC as lost or stolen to TSA as required by 49 CFR 1572.21.6. The individual can present another identification credential that meets the requirements of Section 101.515 of 33 CFR, Part 105.7. There are no suspicious circumstances associated with the individual's claim or loss or theft. | Once fully implemented, the provisions of the Transportation Workers Identity Credential (TWIC) will serve to satisfy the criteria of conducting background checks of U.S. MPTO Employees. | CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements | Not Applicable | <p>CONFLICT: Current state and federal requirements for criminal background checks and issuance of separate access ID cards is confusing to the operators and end users alike.</p> <p>NOTE: Recent alignment of state and federal requirements address the conflicts between the background investigation and permissible ID access card usage requirements. See the TWIC / FUPAC analysis section of this report for further information.</p> |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|---|------------|---|---|---|---|---|---|
| 27. Administration of Statewide Seaport Access Eligibility Reporting System (AERS) - FS 311.12 (5) (a) Subject to legislative appropriations, FDLE shall administer a statewide seaport access eligibility reporting system (AERS). The system must include, at a minimum: 1. A centralized, secure method of collecting and maintaining fingerprints, other biometric data, or other means of confirming the identity of persons authorized to enter a secure or restricted area of a seaport. 2. A methodology for receiving from and transmitting information to each seaport regarding a person's authority to enter a secure or restricted area of the seaport. 3. A means for receiving prompt notification from a seaport when a person's authorization to enter a secure or restricted area of a seaport has been suspended or revoked. | | Not Applicable - Not addressed in FS 311.12 (2001) | Not Applicable - TWIC Provisions Apply | Not Applicable - TWIC Provisions Apply | CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements | Not Applicable | |
| 4. A means to communicate to seaports when a person's authorization to enter a secure or restricted area of a seaport has been suspended or revoked. | | 4. A means to communicate to seaports when a person's authorization to enter a secure or restricted area of a seaport has been suspended or revoked. | 4. A means to communicate to seaports when a person's authorization to enter a secure or restricted area of a seaport has been suspended or revoked. | 4. A means to communicate to seaports when a person's authorization to enter a secure or restricted area of a seaport has been suspended or revoked. | 4. A means to communicate to seaports when a person's authorization to enter a secure or restricted area of a seaport has been suspended or revoked. | 4. A means to communicate to seaports when a person's authorization to enter a secure or restricted area of a seaport has been suspended or revoked. | 4. A means to communicate to seaports when a person's authorization to enter a secure or restricted area of a seaport has been suspended or revoked. |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|--|---|--|---|----------------|--|----------------|--|
| 28. Identify & Establish Exempted Areas - FS 311.12 | As determined by the seaport director's most current risk assessment under paragraph (3) (a), any secure or restricted area that has a potential human occupancy of 50 persons or more, any cruise terminal, or any business operation that is adjacent to a public access area must be protected from the most probable and credible terrorist threat. | Not Applicable - Not addressed in FS 311.12 (2001) | Not Applicable | Not Applicable | CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements | Not Applicable | CONFLICT: FS 311.12 requires the establishment of a mechanism to identify and establish exempted areas within the port as determined by the seaport director's most current risk assessment. The state process for this identification is not coordinated to ensure that the results align with the federal requirements, and does not avoid unintended consequences or implied requirements that will have to be assumed by the port. |
| 29. Identify & Establish Secured & Restricted Areas - FS 311.12 (4) | Each seaport listed in S 311.09 must clearly designate in seaport security plans, and clearly identify with appropriate signs and markers on the premises of a seaport, all secure and restricted areas as defined by the United States Department of Homeland Security, United States Coast Guard Navigation and Vessel Inspection Circular No. 03-07 and 49 C.F.R part 1572. The plans must also address access eligibility requirements and corresponding security enforcement authorizations. | Not Applicable - Not addressed in FS 311.12 (2001) | The FSP must ensure that restricted areas within the facility are designated, and are clearly marked to indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of secure. Facility owner or operator may also designate the entire facility as a restricted area. Restricted areas may include, as applicable: 1. Shore areas immediately adjacent to each vessel moored at the facility. 2. Areas containing sensitive security information, including cargo documentation. 3. Areas containing security and surveillance equipment and systems and their controls and lighting systems controls. 4. Areas containing critical facility infrastructure including water supplies, telecommunications, electrical systems, access points for ventilation and air conditioning, manufacturing or processing areas and control rooms. locations in the facility where access by vehicles and personnel should be restricted, areas designated for loading unloading or storage of cargo and stores, areas containing cargo consisting of dangerous goods or hazardous substances. | Not Applicable | CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements | Not Applicable | NOTE: Recent revisions to FS 311.12 require alignment of state and federal definitions for seaport secure and restricted areas. This is designed to eliminate or significantly reduce conflicts associated with the effective identification and implementation of security measures appropriate to the threats, risks, and commercial operations associated with those areas, at each MARSEC level. |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|---|------------|---|--|----------------|---|--|---|
| 30. Identification of Applicable Seaports - FS 311.12 (a) / FS 311.09 (1) | | | | | | | |
| The list of seaports for which FS 311.12 (2009) is applied remains the same as identified in FS 311.09. | | The Florida Seaport Transportation and Economic Development Council is created within the Department of Transportation. The council consists of the following 17 members: the port director, or the port directors of each of the ports of Jacksonville, Port Canaveral, Fort Pierce, Palm Beach, Port Everglades, Miami, Port Manatee, St. Petersburg, Tampa, Port St. Joe, Panama City, Pensacola, Key West, and Fernandina | 33 CFR, part 105, and NVIC 03-03, change 2 applies to all commercial seaports and OCS facilities that are subject to MTSA. | Not Applicable | CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements | The SFI program has been deployed to the following ports for full implementation: 1. Port Qasim, Karachi, Pakistan 2. Puerto Cortes, Honduras 3. Southampton, UK. SFI is being implemented in a limited fashion at the ports of Singapore, Busan, Korea, Salalah, Oman, and Hong Kong. | Conflict: The minimum security standards outlined in the Port Security Compliance Plan - 2001 apply only to the commercial ports identified in FS 311.09. However, MTSA and the applicable federal minimum security standards and guidance for their implementation is applicable to a number of commercial maritime facilities that are not subject to the state statute. This creates gaps in the effective implementation of a secure operational environment for all commercial maritime activities within the state. |
| 31. Seaports Security Standards Advisory Council - FS 311.115 / 311.115(5) | | | | | | | |
| The Seaport Security Standards Advisory Council is created under the Office of Drug Control. The council shall serve as an advisory council as provided in s. 20.03(7). At least every 4 years after January 15, 2007, the Office of Drug Control shall convene the council to review the minimum security standards referenced in FS 311.12(1) for applicability to and effectiveness in combating current narcotics and terrorism threats to the state's seaports. All sources of information allowed by law shall be used in assessing the applicability and effectiveness of the standards. | | Not Applicable - Not addressed in FS 311.12 (2001) | Not Applicable | Not Applicable | CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements | Not Applicable | Conflict: The existing state and federal security standards and practices is significantly different. This creates challenges when seeking to align state and federal requirements to ease implementation and enforcement practices. However, state adoption of the seaport security performance guidelines identified in NVIC 03-03, change 2 transforms USCG Guidelines into Florida law mandated for implementation by the state legislature. |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|--|---|---|--|---|--|-----------------------|--|
| 32. Maritime Domain Security Awareness Training Program - FS 311.123 | <p>The Florida Seaport Transportation and Economic Development Council, in conjunction with the Department of Law Enforcement and the Office of Drug Control, shall create a maritime domain security awareness training program to instruct all personnel employed within a seaport's boundaries about the security procedures required of them for implementation of the seaport security plan required. The training program curricula must include security training required pursuant to 33 CFR part 105, and must be designed to enable the seaports to meet the training, drill, and exercise requirements of 33 CFR part 105, and individual seaport security plans, and to otherwise comply with the requirements of 311.12.</p> | <p>The Florida Seaport Transportation and Economic Development Council, in conjunction with the Department of Law Enforcement and the Office of Drug Control, shall create a maritime domain security awareness training program to instruct all personnel employed within a seaport's boundaries about the security procedures required of them for implementation of the seaport security plan required. The training program curricula must include security training required pursuant to 33 CFR part 105, and must be designed to enable the seaports to meet the training, drill, and exercise requirements of 33 CFR part 105, and individual seaport security plans, and to otherwise comply with the requirements of 311.12.</p> | <p>The FSP must identify policies and procedures in place to ensure that all personnel, including contractors whether part-time, full-time, temporary or permanent, have knowledge of, through training or equivalent job experience in the following measures as appropriate.</p> <ol style="list-style-type: none"> 1. Relevant provisions of the Facility Security Plan (FSP) 2. the meaning and consequential requirements of the different Maritime Security (MARSEC) Levels as they apply to them, including emergency procedures and contingency plans. 3. Recognition and detection of dangerous substances and devices. 4. Recognition of characteristics and behavioral patterns of persons who are likely to threaten security. 5. Techniques used to circumvent security measures. 6. Familiarity with all relevant aspects of the TWIC program and how to implement them. | <p>A security awareness program should be established and maintained by the MPTO to recognize and foster awareness of security vulnerabilities of the port, vessels and maritime cargo. On an annual basis, employees must be made aware of the procedures the MPTO has in place to report a security concern or incident. Annual refresher training on security and threat awareness should be developed and administered to all employees. Additionally, specific training should be offered on an annual basis to assist employees in maintaining port security vessel and cargo integrity, recognizing internal conspiracies and protecting access control.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable</p> | <p>Overlap/Redundancy/Inefficiency: State and federal requirements for training of port personnel with and without specific responsibilities differ, which may cause:</p> <ol style="list-style-type: none"> 1. Overlap in training programs to achieve compliance with state and federal requirements. 2. Redundancy in areas where the subject matter addressed in the state and federal curriculum for instruction is sufficiently similar that it constitutes additional unnecessary training. 3. The cost of training facility personnel, both in man-hours expended and monies expended for training programs that are not coordinated to simultaneously meet both state and federal requirements is not cost effective. |

| F.S. 311 (2009) | 311.09/311 | PORT SECURITY STANDARDS - COMPLIANCE PLAN F.S. 311.12 (2001) | MTSA 2004 (CFR, Part 105 & NVIC 03-03, Ch 2) | C-TPAT | CSI | SFI | Overlap / Redundancy / Conflicts / Inefficiencies |
|---|------------|--|---|--|--|-----------------------|---|
| 33. Trespassing; detention by a certified seaport security officer - FS 311.12 (3) (a) 2, 3 / FS 311.121 / FS 311.124 | | <p>Any Class D or Class G seaport security officer certified under the federal Maritime Transportation Security Act of 2002 guidelines, and FS 311.121, or any employee of the seaport security force certified under the federal maritime Transportation Security of 2002 guidelines and SF 311.121 who has probable cause to believe that a person is trespassing pursuant to s. 810.09 or this chapter in a designated secure or restricted area pursuant to s. 311.124(4) is authorized to detain such persons in a reasonable manner for a reasonable period of time, pending the arrival of a law enforcement officer. Such action does not render the security officer criminally or civilly liable for false arrest, false imprisonment, or unlawful detention.</p> <p>(2) Upon detaining a person for trespass, the seaport security officer shall immediately call certified law enforcement to the scene.</p> | <p>Facility personnel with specific security duties are required to have general knowledge through training or equivalent job experience in the following security subjects, and the procedures for implementation as identified in the FSP:</p> <ol style="list-style-type: none"> 1. Current security threats and patterns. 2. Recognition of characteristics and behavioral patterns of persons who are likely to threaten security. 3. Techniques used to circumvent security systems. 4. Crowd management and control techniques. The FSP will include guidance regarding the authority, policies and procedures for guard force detention of persons suspected of trespass in the port's secured or restricted areas. | <p>Procedures must be in place to identify, challenge, and address trespassers, unauthorized or unidentified persons. If individuals are encountered that appear to be stowaways or absconders from vessels, CBP personnel at domestic must be notified immediately.</p> | <p>CSI Not Applicable at US Ports. NOTE: All CSI ports must comply with ISPS Code requirements</p> | <p>Not Applicable</p> | <p>Conflict (Potential): Depending upon the location of the incident and the composition of the law enforcement presence available to respond (state-certified vs. federally-certified officers) confusion and conflict may result in determining responsibility for the initial custodial action, and the proper transfer of the detained individual.</p> |

2.3 Comparative Analysis

The comparative analysis of the key elements of the standards and compliance requirements of FS 311 and MTSA identifies conflicts that inhibit the successful implementation and oversight of both security regimes.

Security Objective 1: Each seaport shall maintain a security plan approved by the Florida Department of Law Enforcement (FDLE) and the Governor of Florida's Office of Drug Control (ODC) and the United States Coast Guard. [FS 311.12 (2) (b) & 33 CFR, Part 105.120]

FS 311.12 standard requires that each seaport have a security plan, that the plan must be reviewed and approved by FDLE and ODC, and that the plan must include evidence of participation by the Regional Domestic Security Task Force (RDSTF) and the USCG on any revisions.

NVIC 03-03, Change 2 outlines a process and includes a specific format for the creation of an MTSA-compliant Facility Security Plan (FSP). The MTSA FSP must include the following items that are subject to verification by USCG compliance audits:

- Security administration and organization of the facility;
- Personnel Training;
- Drills and Exercises;
- Records and Documentation;
- Response to Changes in MARSEC level;
- Procedures for interfacing with vessels;
- Declaration of Security (DoS);
- Communications (procedures);
- Security Systems and Equipment Maintenance;
- Security Measures for Access Control, including designated public access areas;
- Security Measures for Restricted Areas;
- Security Measures for Handling Cargo;
- Security Measures for Delivery of Vessel Stores and Bunkers;
- Security Measures for Monitoring;
- Security Incident Procedures;
- Audits and Security Plan Amendments;
- Facility Security Assessment (FSA) Reports; and
- Facility Vulnerability and Security Measures Summary (Form CG-6025).

Analysis

Although the intent of the two regulations is the same, historically the content and language required for either plan is sufficiently different as to compel the port to either maintain two separate plans or create a single plan with duplicative entries for areas where each regulation identifies unique content or specific language requirements (e.g. Form CG-6025).¹³

Florida Statute 311.12 (2009) requires coordination between the state

¹³ Ports indicated the necessity to modify facility security plans to accommodate conflicting language or mutually-exclusive requirements. In some cases ports maintain two sets of "books", one each for review by federal and state auditors. For example: The MTSA requires the inclusion of Form CG-6025 that has no corollary with state standards.

and federal agencies with responsibility for oversight of maritime security standards for Florida's commercial seaports. However, interviews with representatives of the ports indicate that an efficient and effective mechanism for alignment of security plan audits, inspections amendments, and approval has yet to be developed. This is a source of confusion for the ports, and is likely to result in conflicts and inefficiencies that will delay the successful modification and approval of these plans.

Under FS 311.12, Florida ports maintain a Seaport Security Plan (SSP), while MTSA requires the creation and maintenance of a Facility Security Plan (FSP). Attempting to align the basic security document required by both regulatory regimes is confusing and inefficient. This may represent an opportunity for FDLE and the U.S. Coast Guard to work together to integrate the requirements and standardize the nomenclature addressed in the two documents.

Security Objective 2: Each seaport will continuously examine threats through a coordinated mechanism involving regional partners and update security plans when appropriate. Effective July 1, 2009, each port will develop and maintain a Director's Ongoing Risk Assessment (ORA). [FS 311.12 (1) & 33 CFR, Part 105.305]

FS 311.12 requires that each Seaport Director be responsible for conducting risk assessments on a quarterly basis to identify changes in the threat and risk profile associated with the port in order to ensure that appropriate protective security systems and procedures are in place, and that the SSP is appropriately amended in a timely basis.

MTSA requires that a reassessment of the security threats be conducted, at a minimum, every five years as part of the FSP revalidation process. Recurring security vulnerability assessments are conducted on an ongoing basis or as may be required based on significant changes in the port's structure, tenants, or operations.¹⁴

MTSA accepts a layered approach to security sufficient to protect against or mitigate the threats and risks that may be reviewed and approved by the U.S. Coast Guard Sector Commander. Although Florida Statute 311.12 (2009) does include language that reflects an intent to harmonize state and federal standards and procedures for conducting risk assessments of the ports in an efficient, effective, and consistent manner.

Analysis

The FS 311.12 requirement for quarterly risk assessments can easily accommodate the MTSA assessment requirement, as long as the methodology and criteria used to evaluate the risk to the port's personnel, facilities and operations are neither unique nor mutually exclusive. Close cooperation between the Seaport Director, the Facility Security Officer, FDLE, and the U.S. Coast Guard Sector Command is not currently occurring to ensure that this mutual requirement is successfully performed.

¹⁴ FS 311.12 requires quarterly risk assessments of the port against which the restricted areas and risk mitigation measures may be determined. Ports consistently voiced their concern that the state-mandated quarterly assessments were an inappropriate use of resources and stated that the federal annual audits were more appropriate guidance is appropriate for when the threat assessment associated with the Facility Security Plan are to be reviewed and/or amended.

Security Objective 3: To ensure an effective and efficient security apparatus, seaports may operate under alternative standards when such standards are threat based and approved. The seaport may be granted equivalency waivers that create alternative means of compliance from the standards when such alternate means do not diminish the safety or security of the seaport based on the ORA. [FS 311.12 (8)].

FS 311.12 (2009) states that Florida's seaports may operate under alternative security standards, as long as the alternate means of compliance does not diminish the safety or security of the seaport and can be verified through the Seaport Director's risk assessments. ODC and FDLE may modify or waive any physical facility requirements contained in the minimum security standards upon a determination that the purpose of the standards has been reasonably met or exceeded by the seaport requesting the modification or waiver.

Port representatives were consistent in reporting that the waiver process, as currently implemented, is time consuming and represents a possible conflict of interest within FDLE. (NOTE: FDLE's role in the waiver process is to collect information on the level of compliance of the alternate security measures against the compliance standards, and reporting their findings to the Domestic Security Oversight Council (DSOC) for its evaluation and determination).¹⁵ The DSOC membership is heavily weighted for state representation, and the port security experience and knowledge of the DSOC has been called into question by many ports.¹⁶ In addition, the Seaport Security Standards Advisory Council has no role in the waiver appeal process.

Standards for compliance with MTSA requirements are performance based and are linked to the identified threats and risks associated with each port. MTSA compliance may be addressed by a layered security solution that includes a combination of infrastructure and procedural measures the U.S. Coast Guard accepts as appropriate for mitigation of the identified threats and risks.

Analysis

Compliance with this security objective is likely to continue to result in conflicts unless, or until, a consensus is developed on an acceptable range of alternative security standards in conjunction with ODC and FDLE for application statewide.

Security Objective 4: FDLE inspectors will examine the security structure and the overall management of security on the port. [FS 311.12(b) & CFR 33, Part 105.305]

FS 311.12 inspection elements include requirements for:

- Creation of a standing port security committee [FS 311.12 (b)(1)];
- Creation of a Security Master Plan (separate and distinct from the Seaport Security Plan) [FS 311.12 (b)(2)];
- Creation of a Security Manual/Standard Operations Procedures (SOP), applicable to all port personnel that identifies specific security tasks and responsibilities,

¹⁵ FS 311.115 (2) Exemption – FDLE may exempt all or part of a seaport listed in s. 311.09 from the requirements of this section if they determine that activity associated with the use of the seaport or part of the seaport is not vulnerable to criminal activity or terrorism. FDLE will periodically review such exemptions to determine if there is a change in use. Such change may warrant removal of all or part of the exemption.

¹⁶ Ports were consistent in reporting that the DSOC's lack of port security knowledge and experience creates the situation in which the DSOC looks for FDLE guidance in waiver appeals, thus creating a conflict of interest.

-
- conditions, and performance standards [FS 311.12 (b)(3a)];
 - Development of written SOPs for responding to MARSEC level changes [FS 311.12 (b)(3b)]; and
 - The performance of blast zone analysis, if appropriate [FS 311.12 (b)(3b)].

Corresponding MTSA requirements [33 CFR, Part 105.200; 105.205; 105.210; 105.215;] include but are not limited to:

- FSP documentation of port personnel with specific security duties and responsibilities;
- Written designation of the Facility Security Officers (FSO) and 24-hour contact information;
- Inclusion of procedures for shore leave for vessel personnel and crew rotations;
- Report of all breaches of security and security incidents to the U.S. Coast Guard National Response Center; and
- Documentation that the FSO has the authority and ability to maintain the development and implementation of the FSP.

Analysis

Due to lack of coordination regarding the language and composition of facility security plans, some ports maintain multiple security plan documents that address redundant requirements. This results in inefficiencies in application of the requirements as well as in the use of manpower to ensure that the security plan documentation is maintained.

It is likely that this will continue to result in confusion and frustration for the Port Directors and their FSOs unless, or until, a template and/or guidance on acceptable language is developed through the cooperation of FDLE, the U.S. Coast Guard and port community FSOs.

Security Objective 5: Proper record keeping and documentation of security activities is important to improve security. [33 CFR, Part 105.225]

MTSA has established requirements for facility recordkeeping that includes, but may not be limited to:

- Maintenance of required records in hard copy and electronic formats;
- Records of security training, drills & exercises;
- Reports of breaches of security and security incidents;
- Changes in MARSEC levels;
- Maintenance, calibration, and testing of security equipment;
- Security threats to the port's personnel, facilities, and operations;
- Declaration of Security executed between the port and visiting vessels; and
- Results of annual audits of the Facility Security Plan (FSP).

Analysis

Florida Statute 311.12 (2009) mandates that FDLE auditors will review the documentation required for compliance with MTSA. Attached to this requirement is the implied requirement for FDLE inspection team

personnel to be thoroughly trained in, and have an operational understanding of, the security standards and performance objectives required for compliance with the federal requirements outlined in 33 CFR, Part 105 & NVIC 03-03, Change 2.

Security Objective 6: FS 311.12 and seaport security elements will be implemented, in conjunction with the regulatory requirements of the MTSA. FDLE inspectors will collect and examine all COTP letters, notices of violations, fines, and other evidence of security deficiencies issued by the USCG against the port. [FS 311.12 (9) (b)]

Analysis

The FS 311.12 (2009) requirement is likely to receive resistance from the port directors and their FSOs. Ports consistently indicated their concern over the composition of the FDLE inspection audit team and the possible collection of what is viewed as 'derogatory' information about the audited port's security practices. Since FSPs are designated as Sensitive Security Information (SSI), there is likely to be resistance to having representatives of competing ports – who may be included on FDLE audit teams – from viewing SSI information, or for that matter COTP letters, notices of violations, fines, and other evidence of security deficiencies issued by the U.S. Coast Guard against the port.¹⁷

Security Objective 7: Improve security and reduce security costs by imposing minimum criminal background standards to establish the trustworthiness of those regularly entering secure and restricted areas. FDLE inspectors will verify the existence of the required documents by examining the files of the port agency and tenants. [Florida Legislature Standard 2a]

FS 311.12 requires an FDLE conducted criminal background check as a predicate to issuance of a Florida Port ID.

Navigation and Vessel Inspection Circular (NVIC) No. 03-07 identifies the requirements and guidelines for the issuance of a Transportation Worker Identification Credential (TWIC), which includes a national agency, (e.g. FBI, DEA, CIA, etc.), background check conducted by federal authorities to determine suitability for issuance of this credential.

Analysis

The requirement to conduct what is viewed as redundant (e.g. state and federal) criminal background checks has emerged as a contentious lightning rod of discontent among the various port and supply chain community personnel requiring access to the port. Ports consistently reported that the state requirement for the FDLE-conducted background check is an unnecessary bureaucratic mechanism for generating revenue for the state. It is also believed to be an impediment to port community growth and economic development, and a barrier to smooth and efficient commerce with Florida's ports.

Security Objective 8: The seaport shall allow only individuals that can meet a high level security background check. Regular access to secure or restricted areas of the port and shall reduce seaport threat by allowing only such trusted individuals unescorted access into secure or restricted

¹⁷ FDLE's audit teams often include representative of other competing Florida ports. The ports interviewed expressed their concern that inclusion of representatives from other ports compromises the port's SSI. Concern was also expressed by port security personnel, who participated in FDLE audits of other ports, that the prescriptive security standards outlined in 2001 Compliance Plan Inspection Methodology were inconsistently interpreted for application at Florida's ports.

areas. The granting of access eligibility under FS 311.12 must meet certain standards to ensure that only trusted individuals have regular unescorted access to the seaport : [FS 311.12 (7) (a)]

FS 311.12 identifies the criteria for disqualifying offenses associated with the FDLE-conducted criminal background check. FS 311.12 also identifies the time frame the background check covers relative to the applicant's conviction of or release from incarceration, or any supervision imposed as a result of sentencing for committing any of the disqualifying crimes.

The disqualifying offenses for issuance of Florida Port ID include, but may not be limited to:

- An act of terrorism as defined in s. 775.30;
- A violation involving a weapon of mass destruction or a hoax weapon of mass destruction as provided in s. 790.166;
- Planting of a hoax bomb as provided in s. 790.165;
- A violation of s. 876.02 or 876.36;
- A violation of s. 860.065;
- Trafficking as provided in s. 893.135;
- Racketeering activity as provided in s. 893.03;
- Dealing in stolen property as provided in s. 812.019;
- Money laundering as provided in s. 896.101;
- Criminal use of personal identification as provided in s. 817.568;
- Bribery as provided in s. 838.015;
- A violation of s. 316.302, relating to the transport of hazardous materials;
- A forcible felony as defined in s. 776.08;
- A violation of s. 790.07;
- Any crime which includes the use or possession of a firearm;
- A felony violation for theft as provided in s. 812.014;
- Robbery as provided in s. 812.13;
- Burglary as provided in 810.02;
- Any violation involving the sale, manufacture, delivery or possession with intent to sell, manufacture or deliver a controlled substance;
- Any offense under the laws of another jurisdiction that is similar to an offense in this list; and
- Conspiracy or attempt to commit any of the listed offenses.

NVIC 03-07, Guidance for the Implementation of the Transportation Worker Identification Credential (TWIC), identifies the standards for qualification, the criteria for disqualification, and the waiver process procedures for the TWIC.

Analysis

Although the current criminal background checks performed by state and federal investigators are evaluated against differing standards, two background investigations are unnecessarily redundant. Amendment 169 to federal legislation (H.R. 2200) has been initiated by Congresswoman Kathy Castor (FL-11) to direct the Secretary of the Department of Homeland Security to prohibit states from requiring separate security background checks for transportation security cards

and to waive application of the prohibition if a compelling homeland security reason prohibits conducting state or local criminal background checks, or charging for state or local criminal background checks for people who have been issued a TWIC.

Security Objective 9: Any person seeking authorization for unescorted access to secure and restricted areas of a seaport must possess a valid federal TWIC, unless waived. FDLE shall establish a waiver process for an individual who does not have a TWIC, has not obtained a TWIC through a federal waiver process, or is found to be unqualified under FS 311.12 and denied employment by a seaport or unescorted access to secure or restricted areas. [FS 311.12 (7) (e)]

FS 311.12 requires personnel to undergo a Florida Ports ID for unescorted access into restricted areas at Florida's ports to possess a valid TWIC as a predicate for entry into those areas.

Analysis

This requirement, as it is currently implemented, is a bureaucratic redundancy that exists solely to generate revenue for the state of Florida. The current waiver process is viewed as unnecessarily complicated and time consuming, and unresponsive to the operational needs of the seaports and their tenants.

Several ports indicated that the criteria for issuance of a Florida Port ID established by the Legislature is not aligned with TWIC requirements, thus resulting in additional operational inefficiencies.¹⁸

Security Objective 10: FDLE shall administer a statewide seaport Access Eligibility Reporting System (AERS). The system must, at a minimum, include:

- A centralized secure method of collecting and maintaining fingerprints and other biometric data;
- A means of confirming the identity of persons authorized to enter a secure or restricted area of a seaport;
- A methodology for receiving from and transmitting information to each seaport regarding a person's authority to enter a secure or restricted area of the seaport;
- A means for receiving prompt notification from a seaport when a person's authorization to enter a secure or restricted area of a seaport has been suspended or revoked; and
- A means to communicate to seaports when a person's authorization to enter a secure or restricted area of a seaport has been suspended or revoked. [FS 311.12 (5) & (6)]

Analysis

A mechanism to implement the AERS has not yet been developed or aligned with technology and practices associated with the collection, transmission, and use of biometric data collected for issuance of a TWIC credential.

NVIC 03-07 states that the U.S. Coast Guard will conduct continuous vetting on all TWIC holders throughout the 5-year life of the credential;

¹⁸ Federal legislation has been introduced by Hon. Cathy Castor (FL-11) that, if passed, would prohibit the conduct of state criminal background checks for issuance of port access identification for persons having had a federal background check successfully conducted, i.e., TWIC

that the Transportation Security Agency (TSA) will revoke the credential based on any subsequent disqualifying event; and that the TWIC holder will be notified via mail. In addition, if information exists or is developed that a person is an imminent threat, the information will be shared with appropriate parties (e.g., employer, facility or vessel owner/operator, COTP, or law enforcement).

Ports consistently expressed their concern that implementation of the AERS fee requirement prior to the development and functional implementation of the AERS system is premature and could result in a legal challenge. In addition, the AERS system is not compatible with the TWIC reader technology required by federal regulation and may result in the inefficient and costly acquisition and use of two access control technologies.

Security Objective 11: Critical and Sensitive Security Information should be protected to limit the ability of individuals to use the information for criminal or terrorism purposes. [Florida Legislative Standard B6 & 49 CFR, 1520]

This FS 311.12 (2009) requirement corresponds to the requirements outlined in 49 CFR, Part 1520 – Protection of Sensitive Security Information (SSI). This regulation allows the U.S. Coast Guard to maintain national security by sharing unclassified information with various vessel and facility personnel without releasing SSI to the public. SSI includes security assessments and plans, or amendments that contain information, which if released to the general public, would compromise the safety or security of the port.

Analysis

No ambiguity exists between state and federal compliance and oversight authorities regarding this security objective as long as 49 CFR 1520 is the standard used to define SSI, and FDLE implements the applicable procedures as written.

Security Objective 12: The seaport must implement measures to ensure that unauthorized individuals cannot easily defeat locking systems; key control must be implemented. The key control plan must be comprehensive and aimed at protecting the port from unauthorized issuance and copying of keys to port facilities. [Florida Legislative Standard A 10 a]

The Port Security Standards Compliance Plan identifies the key control program elements in order for the port to be considered 'in compliance' with FS 311.12. These standards and practices are also required for inclusion in the MTSA-mandated FSP as an item for inspection by the U.S. Coast Guard facility security compliance inspection team.

Security Objective 13: In order for seaport security infrastructure to meet the public safety objectives required, the security infrastructure must be properly and continuously maintained. Both FS 311.12 and MTSA [Florida Legislative Standard A 10 & 33 CFR, part 105.250] require that:

- There is an adequate system for maintenance of protective security infrastructure and systems;
- Maintenance inspections are regularly scheduled and conducted;
- Infrastructure security components including, but not limited to, fencing, barriers lighting, signage, CCTV

-
- monitoring, intrusion detection, and communications systems are kept in good working order;
 - All security systems and equipment are regularly calibrated and tested;
 - The personnel responsible for use of the security systems and equipment are sufficiently trained to support their efficient and effective use of the systems or equipment; are capable of properly recalibrating the equipment; and are able to perform basic corrective actions in the event equipment performance falls below the required operational parameters; and
 - All of the above information is maintained in the FSP, which is amended by the FSO in the event there is a significant change (e.g. improvement or increased vulnerability) to the security infrastructure.

One of the challenges faced in the alignment of FS 311.12 and MTSA security infrastructure standards is the prescriptive nature of the material, construction, and performance requirements identified in the FS 311.12 Port Security Standards Compliance Plan against the more flexible performance-based standards accepted by the U.S. Coast Guard for compliance with MTSA.

Many port personnel were unaware of the changes in FS 311.12 (2009) to facilitate alignment between the state and federal compliance requirements, specifically the mechanism for requesting equivalency waivers to the prescriptive security standards outlined in the *2001 Port Security Standards Compliance Plan*.¹⁹ Examples of these prescriptive security measures that may be addressed through equivalency waivers include:

- **Fencing:**
 - Fencing should establish a secure perimeter with controlled access;
 - Fencing should be eight-feet high, constructed of nine-gauge galvanized steel, of two-inch wide chain link construction topped with an additional two-foot barbed wire outrigger consisting of three strands of nine-gauge galvanized barbed wire at a 45 degree outward angle above the fence;
 - Bottom of fencing should be no more than two inches from hard surface of concrete or asphalt. This surface should be sufficiently thick to prevent access from underneath; and
 - The exterior and interior sides of the fence should be cleared and uncluttered by not less than five feet to ensure the integrity of the fence is not compromised.
- **Gates/Gate Houses:**
 - Gates and gate houses should be staffed or locked at all times; and
 - The construction of the gates should at least match the construction on the perimeter or interior fencing in general (see fencing above).

¹⁹ FDLE states that no plan is in place for outreach and education to the ports to ensure their understanding of the changes in FS 311.12 or the impact of FDLE expectations regarding acceptable measures to support compliance during the annual audits.

▪ **Lighting:**

- Lighting should be high-mast, sufficient for adequately illuminating exterior gates, piers, cargo areas, cargo traffic areas, and all working and walking areas;
- Lighting should be sufficient to adequately illuminate port operations and cargo areas (e.g. five-foot candles of illumination in dock work areas, including container unloading and loading areas, and one-foot candle of illumination in container/cargo yards).
- Lighting should be directed downward, away from guards or offices, and should produce high contrast with few shadows;
- Updated lighting technology, such as high pressure sodium, mercury vapor, or metal halide lighting, should be used; and
- Lighting must be provided from sunset to sunrise.

Analysis

Dissatisfaction and non-compliance will continue with the requirements outlined in the *2001 Port Security Standards Compliance Plan* until an effective 311.12 (2009) outreach and education program for seaport directors and security staff is developed and implemented. This may require modification of FDLE's role as the agency responsible for audit of port compliance with the mandated security standards to include proactive outreach and education.

Active cooperation between FDLE, the U.S. Coast Guard, and Florida port security management personnel is required to ensure ports are aware of and understand the measures supporting the alignment of state and federal physical security standards, the processes for application and award of security equivalency waivers, and the development of a range of acceptable alternative risk mitigation measures.

Security Objective 14: Ports may use a port agency law enforcement organization to meet security needs. If the seaport creates a law enforcement agency the following inspection elements apply [FS 311.12 (1); 311.12 (8) (C); 311.122 (2)]:

- Waivers for seaport law enforcement personnel standards may not be granted for percentages below ten (10) percent; and
- FDLE inspectors will obtain the necessary records and documentation to ensure the port law enforcement agency meets the required standards for an agency.

The *2001 Port Security Standards Compliance Plan* mandates that port management take steps to ensure the routine, scheduled presence of security patrols by sworn law enforcement personnel, and that port management work with local authorities to negotiate for the permanent assignment of full-time law enforcement officers.

The FS 311.12 (2009) requires there be at least one state certified law enforcement officer assigned to the port on all shifts; that the assigned law enforcement officers have MTSA-mandated maritime security awareness training; and that any waivers granted for law enforcement personnel be below ten (10) percent of the assigned force.

Analysis

Compliance with this state requirement for a law enforcement presence at certain ports has been one of the most costly and problematic issues for port directors and their operating budgets. Many ports have found that the cost of maintaining a sworn law enforcement presence by contracting with the local municipality has significantly increased the percentage of their total operating budget expended for security. In addition, some ports have contracted with their supporting municipalities for a dedicated law enforcement presence which, due to their charter as a department of that municipality, must continue to respond to calls outside the port, making them less-responsive to the port's routine security requirements.

Many ports, especially those engaged in cruise or high-value cargo container operations, have access to layers of federally certified law enforcement officers (e.g. CBP, ICE, U.S. Coast Guard, TSA, etc.), who are very familiar with port operations and may be referenced in the port or terminal's FSP. This reference to the role and function of federal law enforcement personnel at the port is documented in the MTSA-

mandated Area Maritime Security Plan (AMSP), which is managed by the Coast Guard Sector Commander responsible for oversight and enforcement of the security requirements within his/her sector. Unfortunately, since these federal law enforcement officers are not dedicated to security patrol functions and are not accredited by the state of Florida, their presence at the port and inclusion in the FS 311.12 directed SSP does not meet the FDLE standard for compliance with FS 311.12.

This is one of the areas where the Florida ports may realize some economies of scale and efficiencies of operations by having the state statute amended to recognize the presence of federally certified law enforcement officers.

Security Objective 15: Security Guards are a critical human component of the port security apparatus. The port should effectively select and train or ensure the training of a highly competent security guard force that is adequate in quality to perform the necessary security tasks on the port. [Florida legislative standard B 5 b & 33 CFR, Part 105.210; 105.215; 105.220]

FS 311.12 is very specific about the training and certification requirements for contract security personnel performing security duties at Florida's ports. Guard and security personnel must be state certified Class D license holders, while non-sworn security personnel working for a local law enforcement agency and assigned to the port do not require a Class D license. Guard and security personnel whose duties and responsibilities require their use of a firearm must be state certified class G license holders.

MTSA requires that port personnel with specific security responsibilities, as identified in each port's FSP, are required to have knowledge or appropriate training in the following security subjects, some of which will be specific to the port and its operations:

- Knowledge of current security threats and patterns;
- Recognition and detection of dangerous substances and devices;
- Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
- Techniques used to circumvent security measures;
- Security related communications;
- Knowledge of emergency procedures and contingency plans;
- Operation of security equipment and systems;
- Testing, calibration, and maintenance of security equipment and systems;
- Inspection, control, and monitoring techniques;
- Relevant provisions of the port's FSP;
- Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores;
- The meaning and the consequential requirements of the different MARSEC levels; and
- Familiarity with all relevant aspects of the TWIC program and how to carry them out.

All other facility personnel are required to have security training in the following subjects:

-
- Relevant provisions of the port's FSP;
 - The meaning and the consequential requirements of the different MARSEC levels;
 - Recognition and detection of dangerous substances and devices;
 - Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
 - Techniques used to circumvent security measures; and
 - Familiarity with all relevant aspects of the TWIC program and how to carry them out.

The MTSA security training requirement also applies to the sworn and non-sworn law enforcement personnel assigned to the port.

MTSA also requires that security drills and exercises must be performed on a regular and recurring basis. The purpose of these drills and exercises is to test the proficiency of facility personnel in assigned security duties at all MARSEC levels, and to validate their effective implementation of the procedures included in their port's FSP. Drills and exercises are also helpful in identifying deficiencies in port's infrastructure, policies or procedures that may result in changes to the port's FSP.

MTSA mandates that drills be conducted quarterly and should focus on an individual element of a port's FSP. Security exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.

MTSA-mandated security exercises may be:

- Full scale or live;
- Tabletop simulation or seminar;
- Combined with other appropriate exercises; or
- A combination of the above.

Analysis

This is an area where close cooperation between each port and its respective U.S. Coast Guard Sector Command may be leveraged to access U.S. Coast Guard and Department of Homeland Security training, drills, and exercise planning resources via AMSC.

Security Objective 16: In order to meet public safety threats, FS 311.12 (2009) exempted areas and two categories of restricted areas will be established on seaports, and in the FSP's in response to threats and vulnerabilities. Secure and Restricted Areas included in the FSPs must be consistent with the statewide minimum standards for FS 311.12, and be approved as part of the FSP. [FS 311.12 (3) (b), (4) / 33 CFR, part 105.260; NVIC 03-03 Change 2]

The *2001 Port Security Standards Compliance Plan* identified the following locations that should be regarded as restricted areas within Florida's commercial seaports for application of the protective security measures mandated by the statute:

- Cargo storage or staging yards;
- Docks/berths;
- Fuel storage or transfer yards; and
- Cruise terminals.

Modifications to FS 311 made in 2006 designated "seaport authorities", other than the seaport directors, as responsible for identifying four

specific types of “restricted areas” within their ports. These areas are identified as:

- Unrestricted Public Access Area;
- Restricted Public Access Area;
- Restricted Access Areas; and
- Secured Restricted Access Area.

FS 311.111, promulgated in 2006, identified requirements for the enforcement of security standards within these categories of restricted areas, as well as for businesses that are operated outside of but adjacent to designated unrestricted public access areas. These additional security standards were focused on protection of the port facilities, personnel, and operations against credible threats of terrorism using methods and principles contained in the following Federal Emergency Management Agency (FEMA) documents:

- FEMA 426: Reference Manual - to Mitigate Potential Terrorist Attacks Against Buildings; and
- FEMA 452: Risk Assessment - A How To Guide to Mitigate Potential Terrorist Attacks Against Buildings.

FS 311.12 (2009) directs the alignment of the state's definitions of “secure” and “restricted access areas” with the MTSA restricted area definitions. Under MTSA, restricted areas are identified as including, when appropriate:

- Shore areas immediately adjacent to each vessel moored at the facility;
- Areas containing SSI, including cargo documentation;
- Areas containing security and surveillance equipment, systems and their controls, and lighting systems controls;
- Areas containing critical facility infrastructure (e.g. water supplies, telecommunications, electrical systems, access points for ventilation and HVAC systems);
- Manufacturing or processing areas and control rooms;
- Locations within the facility where access by vehicles and personnel should be restricted;
- Areas designated for loading, unloading, or storage of cargo and stores; and
- Areas containing cargo consisting of dangerous goods or hazardous substances.

FS 311.12 (2009) directs that any secure or restricted area on a port that has a potential human occupancy of 50 persons or more, any cruise terminal or any business operation that is adjacent to a public access area **must** be protected from the most probable and credible terrorist threat to human life, as determined by the seaport director's most current risk assessment.

While the most recent version of FS 311.12 does not include guidance on the source of security measures and standards appropriate to these facilities, guidance for security standards appropriate for application to restricted areas and businesses operated outside of, but adjacent to, designated unrestricted public access areas, may be drawn from FEMA 426 and FEMA 452, that provides guidance for protection of facilities against credible threats of terrorism.

Note: Under MTSA the “appropriateness” of restricted area identification is determined based on a number of variables, including:

-
- Credible threats and risks associated with those threats to the ports and its operations;
 - Presence of a vessel, and associated operations, at port terminals and berths;
 - Locations and activities of commercial operations within the port; and
 - Value of the materials or operations subject to protection.

The restricted areas in MTSA-regulated ports are subject to adjustment or modification based on changes in the port's threat/risk profile, or changes in the port's structure, tenants, or operations. Under MTSA, any changes that have the potential to impact the port's restricted areas must be identified in the port's FSP.

Analysis

ODC, FDLE, the U.S. Coast Guard, and Florida port directors and security staffs will need to work together to achieve the intent of the Legislature to align state and federal restricted area definitions and associated protective security measures.

Security Objective 17: To provide adequate protection against acts of terrorism, eliminate illegal smuggling of contraband through the port and port conspiracies, and eliminate general crime, including cargo theft, some areas of the port are designated as Secured Areas (SA) based on the ORA, providing for a secure seaport infrastructure specific to the seaport.

FDLE auditors will note that the primary difference in the operation of an SA and Restricted Area (RA) may be that SAs must be secured by a security guard at each point of access at all times, while an RA may have gated, closed, and locked points of access that are not attended by a security guard when they are not in operation.

NOTE: As determined by the seaport director's most current risk assessment report, any secured area that has a potential human occupancy of 50 persons or more, any cruise terminal, or any business operation that is adjacent to a public access area must be protected from the most probable and credible terrorist threat to human life.

Analysis

ODC, FDLE, the U.S. Coast Guard, and Florida port directors and security staffs will need to work together to achieve the intent of the legislature to align state and federal secured area definitions and associated required preventive security measures.

Security Objective 18: To provide adequate protection against acts of terrorism, eliminate illegal smuggling of contraband through the port and port conspiracies, and eliminate general crime, including cargo theft, some areas of the port may be designated as Restricted Areas (RA) based on the ORA and the mandatory designations found in that standard such that:

- This objective provides for a secure infrastructure specific to the designation of RA based on the ORA, providing for a secure seaport infrastructure specific to the seaport; and
- Promotes the flow of legitimate trade and travel.

Individuals who work on the port, seaport employees, and guests must be controlled via restricted areas, and individuals in these areas are required to have the proper level identification card.

Analysis

ODC, FDLE, the U.S. Coast Guard, and Florida port directors and security staffs will need to work together to achieve the intent of the legislature to align state and federal restricted area definitions and associated required preventive security measures.

2.4 Findings & Recommendations

The following list of findings and recommendations originates from the comparative analysis of the impact of the state and federal compliance requirements on Florida's deepwater seaports, including the results of interviews conducted with management and tenant representatives of Florida ports.

Finding 1: Strict adherence to FDLE standards as in the 2001 Port Security Standards Compliance Plan is focused on strict compliance, without regard to the threats, risks, composition, and operations associated with each port.

FS 311.12 (2009) directs ODC, FDLE, and the U.S. Coast Guard to better align FDLE compliance audit standards and procedures with U.S. Coast Guard compliance requirements and processes.

Finding 2: Definitions of what constitutes Secure and Restricted Access areas, and the protective measures required for each, are confusing and need to be addressed.

FS 311.12 (2009) directs the alignment of state and federal definitions of seaport secure and restricted access areas. The July 1, 2009 revisions to FS 311.12 repeal FS. 311.111 Seaport Security Area Designations. FS 311.12 (2009) restricted areas designations are to be realigned with the definitions in U.S. Coast Guard Navigation and Vessel Inspection Circular 03-07 and 49 C.F.R. Part 1572. This has created the situation in which the U.S. Coast Guard guidance presented in NVIC 03-07, has become Florida law. This is contrary to the U.S. Coast Guard's purpose in issuing NVICs, which is a "guidance" document where seaport compliance is subject to COTP interpretation.

The NVIC allows the COTP to designate portions of the port as operating under non-maritime-related activity and to waive the area from MTSA requirements. The position that FDLE has taken with the ports is that such areas are covered by FS 311.12 standards. FDLE, while acknowledging the changes in definitions of a restricted area in the FS 311.12, state that the FS 311.12 compliance plan still contains a standard for the definition of "restricted area" that also applies, thus creating confusion and lack of coherence between FS 311.12 and the FS 311.12 compliance plan written by ODC in 2000.

Finding 3: FDLE inflexibility in accepting alternative security measures designed to address the threats, risks, and operational requirements of ports is creating a financial burden for port directors, and serves as an impediment to commerce for port tenants.

FS 311.12 (2009) establishes a mechanism for use of alternative security measures and issuance of equivalency waivers for the prescriptive security standards identified in the 2001 Port Security Standards Compliance Plan.

Finding 4: FS 311.12 is viewed as an outmoded, redundant regulatory

requirement that conflicts with federal maritime security standards and is a barrier to commerce for Florida's ports and their tenants.

FS 311.12 (2009) addresses a number of the challenges and impediments to commercial maritime operations perceived by Florida's port directors and their security and marketing personnel. However, there has been little time to implement the changes included in the new legislation that are designed to more closely align state and federal security standards and performance objectives since it was enacted in July, 2009.

Finding 5: FDLE's FS 311.12 compliance requirements are "pass/fail" and are not flexible enough to accommodate U.S. Coast Guard-accepted, risk-based performance standards. The document entitled *2001 Port Security Standards Compliance Plan* was incorporated by reference in FS 311.12. The standards contained therein remain non-performance-based, prescriptive, and inflexible.

Finding 6: The FDLE waiver process for prescribed security standards is time consuming, burdensome, costly, inflexible, and confusing to the ports.

Finding 7: FS 311.12 requires the presence of sworn law enforcement in Florida's ports. Therefore, port directors contract with local municipalities to provide a law enforcement presence to conduct patrols of the ports. FDLE has argued that the purpose for the law enforcement presence is for their deterrent value and their ability to respond to a crime.

The use of sworn law enforcement officers to perform security functions at Florida's ports has been extremely costly for Florida's ports. This is considered an open-ended financial burden, and is an ineffective use of city or county law enforcement resources.

Sworn law enforcement officers are traditionally tasked with conducting arrests and responding to criminal incidents; contract security personnel are traditionally tasked with pro-active security functions (i.e., patrolling, credential checks at access points). To use sworn law enforcement officer in the role of security guards squanders a highly trained and expensive resource. Neither FS 311 nor FDLE recognize the presence of federal officers (e.g., TSA, CBP, ICE, USCG), who are often located at the port, as providing a significant deterrent to crime.

Finding 8: Performance of federal and state criminal background checks for ID credentials to gain access to the same facility, with associated costs for each ID credential, is viewed as a significant problem facing port directors and their security staff.

Port employees, tenants, visitors, and personnel engaged in commerce at ports in Florida and surrounding states do not understand why Florida is the only state where they have to pay for an additional criminal background check, as a prerequisite for issuance of a Florida state port ID, when they have already gone through the criminal background check required for the issuance of the TWIC.

This requirement is widely viewed as nothing more than a bureaucratic mechanism to generate revenue for the state and is believed to be an impediment to attracting commercial tenants to Florida's ports.

Federal legislation has been initiated to prohibit states from collecting fees for criminal background checks for applicants who have already had one conducted under the TWIC requirements.

Page Left Blank Intentionally

3.0 Seaport Security Standards Advisory Council Report & Associated Changes to FS 311 Review

3.1 Introduction

The Seaports Security Standards Advisory Council (SSSAC) was created under the Office of Drug Control (ODC) per F.S. 311.115 to serve the office of the governor as an advisory council as provided in FS. 20.0320. As such, the SSSAC has conducted several studies to assess the status of Florida's seaports and the impact of FS 311.12. The July 30, 2008 submission to the Florida Governor's office provides the SSSAC's recommendations regarding the applicability and effectiveness of FS 311.12. The report provided nine written recommendations and a spreadsheet analyzing the "Minimum Seaport Security Standards."

This section of the Florida Statewide Seaport Security Assessment report will review the recommended changes to FS 311 proposed by the Florida Seaport Security Standards Advisory Council Recommendations dated July 30, 2008 against the existing FS 311.

3.1 SSSAC Recommendation 1

Responsibility for and timely revision of FS 311.12. Florida Legislature should assign responsibility to the SSSAC for the ongoing review of FS 311.12 to ensure the law remains current and minimum seaport security standards are aligned with the federal Maritime Transportation Security Act of 2002 (MTSA), supporting guidance in CFR 33 part 105 and NVIC 03-03 Change 2, and the seaport security requirements of Florida. This would allow additions, deletions, or other modifications pertaining to the law and minimum standards. The Council decided not to submit a White Paper on this subject.

Analysis

- **SSSAC Membership:** The SSSAC, in its current configuration, does not accurately represent the composition of the Florida port community and supporting constituency. Of the 13 members, nine are represented by state officials. Due to the unbalanced membership of the SSSAC, stakeholder input from the private sector is not adequately represented within the SSSAC as currently constituted.
- **Undefined Review Process:** No clearly defined legislative review process of SSSAC actions or decisions is in place. This lack of a review process results in no commentary period and

²⁰ (Online Sunshine, 2009)

does not ensure that the SSSAC is informed of legislative intent toward their actions in a timely basis.²¹

3.2 SSSAC Recommendation 2

“Shall” vs. “Should” Language. Request the Legislature clarify intent regarding use of the word “should” in the minimum standards. The Florida Department of Law Enforcement (FDLE) and the Attorney General provided opinions on interpreting “shall” versus “should” at enclosures 3 and 4; respectfully, Attorney General Position Paper and Florida Department of Law Enforcement (FDLE) Response.

Analysis

The word *should* is used to express a request or condition²². The word depicts the past of *shall* and is used in auxiliary function to express a condition. Use of the word *should* in the Minimum Security Standards for Florida Seaports stipulates procedures utilizing the word “should” (i.e., “should maintain gate passes,” “access to the restricted area should require ...”, “port managers should formally ...”).

The use of the term “should” in FS 311.12 standards is currently understood to imply a discretionary obligation rather than a mandate. While FS 311.12 requires FDLE to evaluate compliance with the Security Standards, inspection teams are accorded no leeway in evaluating digression from the standard. The use of alternate words such as “must,” “shall” or “will” in order to prescribe a mandate will remove ambiguity.

Enclosure 3²³ is provided in the below email from FDLE's

Port Security Email: 10/15/2007

The Attorney General Opinions Section has recently indicated its belief that “should” as used in the statewide minimum seaport security standards does not equate with “shall” and as such is not mandatory.

This position has produced numerous inquiries regarding how this affects the role of the Florida Department of Law Enforcement as it meets its statutory obligations under Chapter 311. FDLE is of the opinion that the determination of whether a seaport is in substantial compliance, mere compliance or is not in compliance of the state's seaport security standards is not affected by whether a standard is “mandatory” or “not mandatory.” FDLE's determination of compliance is a factual and qualitative assessment, regardless of the mandatory or non-mandatory nature of the standard or standards under consideration.

FDLE's inspections and assessments of the degree of compliance will continue to be made as they have been in the past. Seaports will still have the statutory option to request a review by the Domestic Security Oversight Council. Ultimately, the findings of FDLE will be reported to the Legislature.

We believe that the standards continue to represent the minimum level of security expected by the state for each of the affected seaports.

If you have any questions, please call Special Agent in Charge Tom McInerney at (850) 410-6390.

Figure 1: Enclosure 3 - from SSSAC report June 30, 2008

²¹ A member of the SSSAC reported, that due to the makeup of the SSSAC, state of Florida votes on the council far outweigh port industry votes.

²² <http://www.merriam-webster.com/dictionary/should> Merriam Webster online Dictionary, (2009) Accessed: November 12, 2009

²³ SSSAC RECOMMENDATION REPORT June 30, 2008: Enclosure 3: Attorney General Position Paper

Commissioner Bailey in which FDLE – while recognizing the Attorney General's statement that the ambiguity present in the use of "shall" vs. "should," statute language has caused "inquiries" regarding the role of the FDLE – has indicated to the ports that it will abide by a strict interpretation that the standards are required, and are not optional.

3.3 SSSAC Recommendation 3

Private ports not addressed by Minimum Standards. *Although the Council was not asked to address private commercial seaports, there was considerable concern regarding the number of private commercial seaports and the lack of similar state standards to ensure implementation of effective preventive security measures for their operation.*

Analysis

Intelligence reports reviewed for this report confirm that private commercial seaports, including the Miami River Seaport, are significant sources of the types of criminal activities FS 311.12 was designed to mitigate. Private commercial seaport security is not addressed by FS 311.12. However, instances do occur within the state of Florida in which a public port is placed at an economic disadvantage when compared to a competing public port. In this instance, the private port is held only to the MTSA, while the public one is held to both FS 311.12 and the MTSA. In the case of two closely placed ports, commerce would arguably flow to the port held to a nationwide standard only.

3.4 SSSAC Recommendation 4

Transportation Worker Identification Credential (TWIC). *The Council frequently discussed federal and state port access credentials. The duplication of enrollment and the costs of the programs were most often discussed. The Council did not recommend any reduction in Florida standards, but did recommend alignment of the two credentials into a single credential.*

Analysis

Participants in this study, consisting of port directors, port security directors and FDLE representatives, were consistent in reporting port tenant and port worker confusion and frustration regarding TWIC and Access Eligibility Report System (AERS) implementation.

The Legislature, through House Bill (HB) 7141, addressed this concern in updating security provisions for the state's seaports. HB 7141, among other actions, created the Access Eligibility Reporting Systems (AERS), and eliminated the Florida Uniform Port Access Credential (FUPAC). HB 7141 also states the Legislature's following intent to:

- Establish TWIC as the only credential authorized for use by the seaports listed in s. 311.09, F.S.;

-
- Maintain a requirement for a criminal history background check of crimes committed in Florida when determining access eligibility for secure and restricted areas at Florida's commercial seaports identified in FS 311.09; and
 - Align state criminal offenses that disqualify a person for unescorted access to secure and restricted access areas with federal disqualifying offenses under the TWIC program, and create an affidavit process for determining access eligibility for TWIC holders that reduces and consolidates state fees for port workers.

Despite the recent changes to FS 311.12, the following has occurred:

- Additional disqualifying factors still exist under the AERS, which indicates that the AERS and the TWIC, while more streamlined, are not yet completely aligned, thus creating confusion in the port community;
- For TWIC holders, FDLE requires a background check against Florida's criminal history databases. FDLE requires non-TWIC holders who require regular access to restricted or secure areas of the port, whether escorted or not, to submit to both national and state background checks; and
- At the time of writing, the AERS has not been implemented. This is due, in large part, to the passage of legislation prior to the completion of a full implementation plan including related technology and training.

3.5 SSSAC Recommendation 5

Federal Presence. *The Council noted that since the September 11, 2001 attack on America, Florida's seaports have become more secure due to increased federal presence. The U.S Coast Guard's terrorism-focused risk assessment, in conjunction with other Federal agencies' focus on criminal activities, has synergistically enhanced port security. They have accomplished this by simultaneously addressing terrorism, drug trafficking, cargo theft and crime.*

Analysis

It is apparent that federal efforts to secure U.S. transportation infrastructure systems and facilities have multiplied exponentially over the last decade. The government's multi-layer security strategy is sound, and addresses cargo and maritime security on national and international basis. Security issues are no longer addressed for the first time when a ship and its cargo arrive at a U.S. port.

Since it was established in 2002, the Department of Homeland Security (DHS) has integrated a number of component agencies that have responsibility for oversight and enforcement of preventive security measures for the country's transportation infrastructure, including America's commercial maritime industry.

The U.S. Coast Guard is the primary federal agency responsible for port security. The U.S. Coast Guard is charged with protecting the public, the environment, and U.S. economic and security interests in any maritime region that may be at risk, including U.S. coasts, ports, and inland waterways.

The Transportation Security Administration (TSA) is the federal agency responsible for securing transportation systems, including those located at the ports.

U.S. Customs and Border Protection (CBP) has prioritized denying entry into the U.S. by a variety of external threats, including criminal and terrorist, and their weapons or other contraband. CBP is responsible for securing and facilitating trade, and has the primary responsibility for implementing cargo container security programs.

A complete review of the federal impact on security within the state of Florida can be found in Section 4 of this report.

3.6 SSSAC Recommendation 6

Seaport Security Plan Language. Request the Legislature clarify intent regarding the enforcement of Florida-specific requirements contained in the Seaport Security Plan. Discussions during the meetings included concern that the Seaport Security Plan enforcement currently is a U.S. Coast Guard function. This leaves the impression that the U.S. Coast Guard was meant to enforce Florida state standards.

Analysis

Since FS 311.12 Section (3) *Security Plan* was revised on July 1, 2009, the SSSAC concern regarding U.S. Coast Guard enforcement of FS 311 is no longer an issue. Recent modifications now define the process, timeline and partners for the creation and review of port security plans. Security plans, under the revised FS 311.12, are now evaluated for both FS 311.12 and MTSA compliance by the FDLE, with a copy of the results of said evaluation provided to the U.S. Coast Guard. A new situation has been created in which a state entity, in this case FDLE, is charged with evaluating compliance with the MTSA. It is unclear if FDLE have the training or background knowledge to do so.

3.7 SSSAC Recommendation 7

Alignment of Federal and State "restricted areas." Request the Legislature review the provisions of FS 311.111 for possible alignment with the federal Security Area Definitions, yet maintain the seaport security requirements as needed by the state of Florida. The review should also balance requisite security requirements with seaport commerce.

Analysis

The July 1, 2009 revisions to FS 311.12 repeal FS. 311.111 Seaport Security Area Designations. FS 311.12 (2009) restricted areas designations are to be realigned with the definitions in U.S. Coast Guard Navigation and Vessel Inspection Circular 03-07 and 49 C.F.R. Part 1572. This has created the situation in which the U.S. Coast Guard guidance present in NVIC 03-07, has become law in the state of Florida. This is contrary to the U.S. Coast Guard's purpose in issuing NVICs, which is a "guidance" document, with seaport compliance subject to COTP interpretation.

The NVIC allows the COTP to designate portions of the port as operating under non-maritime-related activity, and to waive the area from MTSA requirements. The position that FDLE has taken with the ports is that such areas are covered by FS 311.12 standards. FDLE, while acknowledging the changes in definitions of a restricted area in the FS 311.12, state that the FS 311.12 compliance plan still contains a standard for the definition of 'restricted area' that also applies, thus creating confusion and lack of coherence between FS 311.12 and the FS 311.12 compliance plan written by ODC in 2000.

3.8 SSSAC Recommendation 8

Study language: *The Camber Report of the security of Florida ports was completed in 1999. A new security study of Florida's ports in 2008 is warranted given the time that has passed, the events of 9/11, and the dramatic changes in port growth, operations and security, as well as ongoing criminal activity and the advent of terrorism.*

Analysis

In partial response to SSAC Recommendation 8, a review of the *Camber Report* is presented in Section 1. In addition, Sections 7, 8, and 9 contain current physical, operational, and risk profiles that also serve to address Recommendation 8.

3.9 SSSAC Recommendation 9

Area Maritime Security Committees: *In accordance with FS 311.12, the Council is required to consult with Area Maritime Security Committees (AMSC). Their letter is at enclosure 5, Area Maritime Security Committees' response.*

Analysis

The SSSAC, as evidenced in the following letter, attempted to consult with local AMSCs. Two AMSCs declined to participate. However, the AMSCs that did participate took the following positions:

- Excessive time involved in reviewing FS 311.12 standards;
- The fact that the standards are based on ten year old assessment that ignores industry standards; and

-
- The level of security would be diminished by overlaying a standards-based system on the MTSA-mandated risk-based system.

U.S. Department of
Homeland Security

United States
Coast Guard



Commander (dp)
Seventh Coast Guard District

909 S.E. First Avenue
Miami, FL 33131-3050
Staff Symbol: dpl-7
Phone: (305) 415-6838
Fax: (305) 415-6875
Email: Christian.f.weltler@uscg.mil

16600
June 12, 2008

Mr. Gilbert D. Barnes
Corrections Liaison
Florida Drug Control Office
Office of Governor Charlie Crist
Tallahassee, Florida 32399-0001

Dear Sir:

As you requested on 1 May, 2008, five Florida Area Maritime Security Committees were afforded the opportunity to provide written comments on the proposed changes to FL Statutes 311.11 and 311.12. Below are their consolidated and unedited responses.

1. AMSC Western Florida. "The AMSC membership declined to evaluate individual standards contained in the proposed changes to F.S. 311.12, as submitted. The reasoning includes the time required to adequately evaluate the requested impact properly, and statements by members that commenting on the standards would indicate an approval of a Standards Based system based on a 10 year old assessment that ignores industry standards, such as those promulgated by the American Society of Industrial Security, International.

Additionally, the AMSC, after consideration and discussion, concluded that the Standards Based system utilized by the Seaport Security Administrator, as required by F.S. 311.12, does not align with the Risk Based philosophy adopted by the Coast Guard, and generally accepted by industry.

Several members of the AMSC stated in detail their belief that overlaying a Standards Based system on the MTSA mandated Risk Based system often diminishes the level of security within the Maritime Transportation System.

As an example, cargo storage and staging areas are designated under state requirements by definition in lieu of usage, meaning that if at any time an area is used to hold cargo, it must be protected to that standard at all times. Therefore, full restricted area standards are in force in non-operational areas to meet compliance requirements. An example given was a requirement to light an empty field sometimes used to store cargo to the same standard as if it always contains cargo because it is designated a "cargo storage or staging area" under F.S. 311.12. Because F.S. 311.12 mandates expenditure of security funds to meet the standard, fewer funds are available to implement security measures indicated by risk analysis.

As stated by an AMSC member, F.S. 311.12 requires them to spend their limited security funding poorly."

2. AMSC Panama City "We want only one regulatory agency. We could enumerate a laundry list of draw backs with either agency, but the contradictions and duplications of having to answer to two authorities are causing unnecessary "clutter" for almost all Florida ports."

3. AMSC Florida Keys Declined to submit written comment.

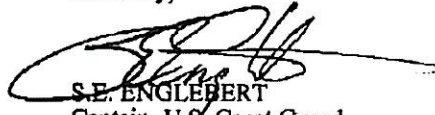
16600
June 12, 2008

4. AMSC Miami Declined to submit written comment.

5. AMSC Northeast and Eastern Central Florida "The Northeast and Eastern Central Florida AMSC declined to comment on the standards contained in the proposed changes to F.S. 311.12 for fear it would lend legitimacy to the State of Florida's claim over it."

Please feel free to contact me if you have any further comments or questions.

Sincerely,


S.E. ENGLEBERT
Captain, U.S. Coast Guard
Chief, Prevention Division
Seventh Coast Guard District
By direction

Copy: Commander, CG Sector Jacksonville
Commander, CG Sector Miami
Commander, CG Sector Key West
Commander, CG Sector St Petersburg
Commander, CG Sector Mobile

Page Left Blank Intentionally

4.0 U.S. Port Security Regulatory Review: 2000 & 2009

4.1 Introduction

After the implementation of FS 311.12 in 2000-2001, and subsequent to the terrorist attacks of 9/11, the federal government began a concentrated effort to bolster security at U.S. seaports in response to CIA and other agencies reporting the increased domestic threat of transnational terrorism.

To provide a foundation for understanding the complex evolution of federal regulations that has evolved since 2000, this section of the report reviews and presents in tabular form a timeline of federal statutory requirements and guidelines (i.e., U.S. Coast Guard, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, etc.). Implemented security measures range from the Maritime Transportation Security Act (2002), the International Ship and Port Facility Security (ISPS) Code, which was heavily influenced by the U.S. Coast Guard (USCG), and regulatory policies and directives, such as U.S. Coast Guard NAVICs.²⁴

It is apparent that federal efforts have multiplied exponentially over the last decade. The government's multi-layer security strategy is sound, and addresses cargo and maritime security on an international basis. Security issues are no longer addressed for the first time when a ship and its cargo arrive at a U.S. port.

Since it was established in 2002, the U.S. Department of Homeland Security (DHS) has implemented numerous component agencies that have responsibility for securing areas of transportation security. The Transportation Security Administration (TSA) is the federal agency with primary responsibility for securing all modes of transportation and has developed and implemented a variety of programs and procedures to secure transportation. U.S. Customs and Border Protection (CBP) has prioritized keeping terrorists and their weapons out of the U.S., is responsible for securing and facilitating trade, and has primary responsibility for cargo container security. The U.S. Coast Guard has responsibility for protecting the public, the environment, and U.S. economic and security interests in any maritime region that may be at risk, including U.S. coasts, ports, and inland waterways.

To provide better illustrate federal maritime security efforts, the following table provides a chronological timeline of maritime security regulations and guidelines that have been issued since 2000.

4.2 Regulatory Measures & Guidelines

| Date | Regulatory Measures & Guidelines |
|------|---|
| 1986 | International Maritime and Port Security Act: Title IX of the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (Pub. L. 99-399; 100 Stat. 889) constitutes the International Maritime and |

²⁴ A Navigation and Vessel Inspection Circular (NVIC) provides guidance about the enforcement or compliance with federal and U.S. Coast Guard marine safety regulations and programs. NVICs are non-directive; they do not have the force of law. Non-compliance with a NVIC is not a violation of the law, however non-compliance may indicate non-compliance with a law, a regulation or a policy. The U.S. Coast Guard uses NVICs internally to ensure that inspections and other regulatory actions are adequate, complete and consistent. Likewise, the maritime industry uses NVICs to learn how the U.S. Coast Guard will enforce regulations or conduct programs. NVICs are issued by the Assistant Commandant for Marine Safety, Security and Environmental Protection.

| | <p>Port Security Act. This act amended the Ports and Waterways Safety Act, which then provided the U.S. Coast Guard authority to "carry out or require measures, including inspections, port and harbor patrols, the establishment of security and safety zones, and the development of contingency plans and procedures, to prevent or respond to acts of terrorism." This law also required a proposed plan of action for implementation of security measures at U.S. ports and passenger vessels operating from those ports.</p> | | | | | | | | | | | | | | |
|-----------------|--|------|---------------------------|------|-----|------|-----|------|-------|------|-------|------|-------|------|-------|
| 1993 | <p>NVIC 3-93: NVIC 3-93 describes the procedures required to implement the passenger vessel security regulations of Title 33 CFR parts 120 and 128 (reference [a]). Guidance is provided for processing Terminal and Vessel Security Plans, assessing the adequacy of those plans, and establishing annual reporting requirements, incident reporting, and threat dissemination procedures. NVIC 3-93 called attention to the 1992 Fire Safety Amendments to the International Convention for the Safety of Life at Sea, 1974 (SOLAS 74).</p> | | | | | | | | | | | | | | |
| 1995 | <p>NVIC 4-95: NVIC 4-95 cancelled NVIC 3-93. The objective of this NVIC is to provide foreign passenger vessel owners, operators, and U.S. Coast Guard field units with the additional information and guidance necessary to prepare for the Control Verification Examination process. The increased guidance was designed to ensure consistent enforcement of the 1992 SOLAS Amendments while continuing to minimize delays for vessel owners and operators.</p> | | | | | | | | | | | | | | |
| 2001 | <p>Custom and Trade Partnership Against Terrorism (C-TPAT): C-TPAT was launched in November 2001. It is a voluntary government-business initiative to build cooperative relationships that strengthen and improve overall international supply chain and U.S. border security. Through this initiative, U.S. Customs and Border Protection (CBP) partners with private industry to ensure the integrity of their security practices and communicate and verify the security guidelines of their business partners within the supply chain.</p> <p>Benefits to certified C-TPAT member categories:</p> <ul style="list-style-type: none"> ▪ Reduced Inspections: A reduced number of CBP inspections (reduced border delay times); ▪ Priority processing: Priority processing for CBP inspections. (Front of the Line processing for inspections when possible.); ▪ Assistance and Guidance: Assignment of a C-TPAT Supply Chain Security Specialist (SCSS) who will work with the company to validate and enhance security throughout the company's international supply chain; ▪ Importer Self-Assessment Program: Potential eligibility for CBP Importer Self-Assessment program (ISA) with an emphasis on self-policing, not CBP audits; and ▪ Seminars: Eligibility to attend C-TPAT supply chain security training seminars. | | | | | | | | | | | | | | |
| 2001 (cont.) | <p>C-TPAT Validations/Revalidations Per Year</p> <table border="1"> <thead> <tr> <th>Year</th> <th>Validations/Revalidations</th> </tr> </thead> <tbody> <tr> <td>2003</td> <td>137</td> </tr> <tr> <td>2004</td> <td>294</td> </tr> <tr> <td>2005</td> <td>1,109</td> </tr> <tr> <td>2006</td> <td>2,266</td> </tr> <tr> <td>2007</td> <td>3,092</td> </tr> <tr> <td>2008</td> <td>3,469</td> </tr> </tbody> </table> | Year | Validations/Revalidations | 2003 | 137 | 2004 | 294 | 2005 | 1,109 | 2006 | 2,266 | 2007 | 3,092 | 2008 | 3,469 |
| Year | Validations/Revalidations | | | | | | | | | | | | | | |
| 2003 | 137 | | | | | | | | | | | | | | |
| 2004 | 294 | | | | | | | | | | | | | | |
| 2005 | 1,109 | | | | | | | | | | | | | | |
| 2006 | 2,266 | | | | | | | | | | | | | | |
| 2007 | 3,092 | | | | | | | | | | | | | | |
| 2008 | 3,469 | | | | | | | | | | | | | | |

| | |
|------|--|
| | C-TPAT is not a regulatory program, and it is not a guarantee of security. It does, however, provide for a creative partnership approach between government and industry as one element of a multi-layered strategy to improve security. ²⁵ |
| 2002 | <p>Maritime Transportation Security Act (MTSA) of 2002: The MTSA is a comprehensive port security legislation approved in November 2002. The MTSA required that the following actions be taken:</p> <ul style="list-style-type: none"> ▪ Risk Assessments: The conduct of a risk assessment of vessels and facilities on or near the water to identify those at high risk of attack or accident; ▪ Area Maritime Security Committee (AMSC) Plans: The development of national and area maritime transportation security plans; ▪ U.S. Coast Guard Approval of Facility and Vessel Security Plans (FSP / VSP): The development of security plans by ports, facilities and vessels that are approved by the U.S. Coast Guard. The MTSA, through 33 CFR 105, established a deadline of December 31, 2003 for the approval of all FSPs; ▪ Improved Coordination between Local, State, and Federal Agencies: Better coordination among local port security committees and federal, state, local, and private law enforcement bodies, including intelligence agencies, the FBI, CBP, Immigration, and the U.S. Coast Guard; ▪ Restricted Areas / ID Cards: The development of regulations for secure areas in ports, including ID cards; ▪ Improved Inspections: Research and development grants for improved customs inspection of ships entering the U.S.; ▪ Security Training / Certification: The development of security training and the education / certification of security personnel; ▪ Intelligence System: The development of a maritime intelligence system and the improvement of reporting of crew, passengers, and cargo; ▪ Sea Marshal Program: Authorized the creation of the Sea Marshal program; and ▪ Automatic Identification System (AIS): Equipping commercial vessels with an automatic identification system so that vessels are able to be tracked in U.S. waters. |
| 2002 | <p>Department of Homeland Security (DHS): DHS was created in 2002.²⁶ The rationale was to enhance the synergy and efficiency of homeland security efforts among its various parts. The primary mission of DHS is to:</p> <ul style="list-style-type: none"> ▪ Prevent terrorist attacks within the U.S.; ▪ Reduce the vulnerability of the U.S. to terrorism; ▪ Minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the U.S.; ▪ Carry out all functions of entities transferred to DHS, including natural and manmade crises and emergency planning; and ▪ Monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and contribute to interdiction of illegal drug trafficking. |
| 2002 | <p>U.S. Customs and Border Protection: U.S. Customs, Immigration and Naturalization and Agriculture were reorganized into CBP. CBP is an agency within DHS. CBP consolidated the federal inspection responsibilities related to both the inspection of international cargo and the examination of persons arriving at U.S. maritime ports. CBP, a component of the DHS Directorate for Border and Transportation Security (BTS), is focused on intercepting containers bearing weapons of mass destruction (WMD) and / or crew members / passengers carrying falsified passports. CBP relies on</p> |

²⁵ Testimony of Christopher Koch, President & CEO of the World Shipping Council, regarding maritime and port security before the U.S. Senate Committee on Commerce, Science, and Transportation (2006).

²⁶ Section 101(b) of the Homeland Security Act of 2002.

| | |
|------|--|
| | risk-based "targeting" to identify those containers and ships that present the greatest threat to the U.S. Those high-risk entities are then the focus of CBP inspection efforts. This process requires <i>high quality</i> intelligence to complete the risk analysis. ²⁷ |
| 2002 | U.S. Immigration and Customs Enforcement (ICE): The creation of DHS was also accompanied by the creation of a new investigative / enforcement agency of ICE. ICE is charged with investigating and enforcing the customs and immigration laws at U.S. seaports. As such, the agency participates in many activities that generate homeland security intelligence. ²⁸ |
| 2002 | U.S. Coast Guard: The U.S. Coast Guard was integrated into DHS in 2002. The U.S. Coast Guard has security responsibility for vessels, waterways and port facilities. These security responsibilities are distributed throughout the U.S. Coast Guard, through the various Captains of the Port (COTP), marine security offices and law enforcement operations. |
| 2002 | <p>Container Security Initiative (CSI): In January 2002, the CSI program was created in partial response to the vulnerable seaport situation. The program targets the problem of potentially dangerous containers well before they entered the United States, and consists of four core elements: Establish security criteria to identify high-risk containers; pre-screen those containers before arrival at U.S. ports; use technology to pre-screen high risk containers; and develop the use of smart technology to secure containers.²⁹</p> <p>Under the CSI program, a team of officers is deployed to work with host nation counterparts to target all containers that pose a potential threat. Announced in January 2002, CSI was first implemented in the ports shipping the greatest volume of containers to the U.S. Today, customs administrations all over the world have committed to joining CSI and are at various stages of implementation. CSI is now operational at ports in North, Central, and South America, the Caribbean, Europe, Africa, the Middle East, and throughout Asia.³⁰</p> |
| 2002 | International Ship and Port Facility Security (ISPS) Code: Seeking to widen efforts to increase security for shipping worldwide, the U.S. in early 2002 introduced proposals similar to the MTSA at the U.N.'s International Maritime Organization (IMO). The IMO adopted the ISPS Code in mid-December 2002. The ISPS Code set forth a deadline for implementation on July 1, 2004. |
| 2003 | NVIC 11-02 & 11-02 Change 1: Recommended Security Guidelines for Facilities: This NVIC provides guidance on developing security plans, procedures, and measures for facilities. Until final regulations regarding facility security were published, this Circular was used as a benchmark to develop and implement security measures and activities in anticipation of evolving domestic and international security regimes. |
| 2004 | <p>MTSA of 2004: Amends the MTSA of 2002 to include:</p> <ul style="list-style-type: none"> ▪ Commercial Maritime & Intermodal Curriculum Development: Establish a curriculum to educate and instruct federal and state officials on commercial maritime and intermodal transportation. ▪ Law Enforcement Training: Coordinate with the Federal Law Enforcement Training Center (FLETC) in the curriculum development and the provision of training opportunities for federal and state law enforcement officials at appropriate law enforcement training facilities. ▪ Transportation Worker Identification Credential (TWIC): Directs the DHS Secretary to |

²⁷ Henrikson, A. (2005). *An Interagency Approach to U.S. Port Security. Strategic Insights*, v IV, Issue 2. Accessed from <http://www.nps.edu/Academics/centers/cccl/publications/OnlineJournal/2005/Feb/henriksonfeb05.html> January 31, 2009.

²⁸ Henrikson (2005).

²⁹ Robinson, C. (2003). *Port and Maritime Security in the United States: Reactions to an Evolving Threat*. Center for Defense Information. <http://www.cdi.org/terrorism/maritimesecurity-pr.cfm>. Accessed January 31, 2010.

³⁰ CSI Fact Sheet (2007). http://www.cbp.gov/xp/cgov/trade/cargo_security/csi/csi_in_brief.xml Accessed January, 31, 2010.

| | |
|------|--|
| | <p>report to specified Congressional committees on recommendations to coordinate background checks for all individuals engaged in transportation activities; and a timeline for implementation of TWIC in seaports.</p> <ul style="list-style-type: none"> ▪ Area Maritime Transportation Security Plans: Amends federal shipping law to direct the Under Secretary of Homeland Security for Border and Transportation Security to establish a maritime transportation security plan grant program to implement Area Maritime Transportation Security Plans and help fund compliance with federal security plans among port authorities, facility operators, and state and local agencies required to provide security devices. |
| 2004 | <p>NVIC 06-03 Change 1 Coast Guard Port State Control Targeting and Boarding Policy for Vessel Security and Safety: NVIC 06-03 Change 1 revises Navigation and Vessel Inspection Circular (NVIC) No. 06-03 and includes updated procedures for risk-based vessel targeting, reporting and notification, boarding, and control and enforcement, and revised examination checklists.</p> |
| 2004 | <p>NVIC 06-04 Voluntary Screening Guidance for Owners or Operators: NVIC 06-04 provides guidance to aid owners or operators in the development and execution of a screening regime to meet the requirements of Subchapter H of Title 33, CFR Subchapter H, which requires certain owners or operators of vessels or facilities to conduct screening of persons, cargo, vehicles, or baggage prior to allowing access onto the facility or vessel. The guidance is not provided to regulate owners or operators in the development of a screening program. Owners or operators are not required to use this document in developing a screening program. This guidance is an overview of what owners or operators should consider when establishing a screening program.</p> |
| 2004 | <p>NVIC 10-04 Guidelines for Handling of Sensitive Security Information (SSI): The purpose NVIC 10-04 is to provide guidance to field commanders and the maritime industry on the access, safeguarding, and disclosure of information, designated as SSI, as defined in 49 CFR Part 1520 (as amended). SSI is information that the Transportation Security Administration (TSA) has determined must be protected from improper disclosure in order to ensure transportation security. TSA has amended its SSI regulations to cover the security measures required by the MTSA and exempts information related to maritime security from public disclosure under the Freedom of Information Act (FOIA).</p> |
| 2005 | <p>NVIC 02-05 International Port Security (IPS) Program: NVIC 02-05 outlines the procedures for conducting the International Port Security (IPS) Program. The guidance details the process for conducting information exchanges with other countries to learn how they are implementing the ISPS Code and the actions to be taken in the event that significant implementation problems are discovered.</p> |
| 2005 | <p>National Strategy for Maritime Security: The National Strategy for Maritime Security aligns all federal government maritime security programs and initiatives into a comprehensive and cohesive national effort involving appropriate federal, state, local, and private sector entities. In addition to this strategy, the Departments have developed eight supporting plans to address the specific threats and challenges of the maritime environment. While the plans address different aspects of maritime security, they are mutually linked and reinforce each other. The supporting plans include:</p> <ul style="list-style-type: none"> ▪ National Plan to Achieve Domain Awareness; ▪ Global Maritime Intelligence Integration Plan; ▪ Interim Maritime Operational Threat Response Plan; ▪ International Outreach and Coordination Strategy; ▪ Maritime Infrastructure Recovery Plan; ▪ Maritime Transportation System Security Plan; ▪ Maritime Commerce Security Plan; and ▪ Domestic Outreach Plan. |

| | |
|------|---|
| | <p>Together, the National Strategy for Maritime Security and its eight supporting plans present a comprehensive national effort to promote global economic stability and protect legitimate activities while preventing hostile or illegal acts within the maritime domain.</p> |
| 2005 | <p>Maritime Transportation System (MTS) Security Recommendations: The MTS security recommendations respond to the President's call to improve the national and international regulatory framework regarding the maritime domain. MTS security is an essential component to the National Strategy for Maritime Security. The U.S. must do more to prevent terrorist attacks in the maritime domain, and protect critical infrastructure and key assets which are part of MTS. The MTS security recommendations aim to improve the national and international regulatory framework for all private and commercial operations in the maritime domain. To ensure a holistic solution, the recommendations also address land-based infrastructure and intermodal connections that are vital for moving goods and people across the United States. The recommendation categories include:</p> <ul style="list-style-type: none"> ▪ Risk Management; ▪ Security Information Management; ▪ International & National Regulatory Framework; ▪ Stakeholder Responsibility & Coordination; ▪ Credentialing; ▪ Leverage Safety Frameworks; ▪ Security Technology; and ▪ Security Training. |
| 2006 | <p>Security and Accountability For Every Port Act (SafePort Act): The SafePort Act amends the MTSA to accomplish the following³¹:</p> <ul style="list-style-type: none"> ▪ Regulate Access: Requires vessel and security plans under MTSA to regulate access by engaging in the surface transportation of intermodal containers in or out of a facility; ▪ Resubmission of FSPs and VSPs: Requires the submission of a new vessel and security plan after a change of ownership or operation of a facility; ▪ U.S. Citizenship of Facility Security Officer (FSO): Requires U.S. citizenship for individuals implementing security actions for a facility, but allows a waiver of such requirement after a complete background check and review of terrorist watch lists; ▪ Announced and Unannounced Inspections: Requires verification, at least twice annually, the effectiveness of a VSP and FSP, with at least one of the inspections to be unannounced. ▪ Transportation Security Cards: Imposes additional requirements under MTSA for issuing transportation security cards. ▪ Inefficiencies in Background Checks: Directs the Comptroller General to study and report to Congress on redundancies and inefficiencies in connection with background records checks for DHS. ▪ Interagency Operational Centers: Establishes interagency operational centers for port security at all high-risk priority ports not later than three years of the Act. Describes required characteristics. Designates the U.S. Coast Guard COTP in an operational center as the incident commander in the event of a transportation security incident; ▪ Maritime Risk Assessment Model (MSRAM): Makes available a risk assessment tool that uses standardized risk criteria for updating area maritime security plans and for applying for port security grants. ▪ Port Security Grants: Requires the allocation of port security grants based on risk. Limits the use of grant funds for construction costs. Expands eligible costs under such grant program to include: <ol style="list-style-type: none"> 1. Exercises: Training exercises relating to terrorism prevention or recovery; 2. Information Sharing: Sharing of terrorism threat information; and 3. SSI Storage Costs: Equipment costs for storing classified information. |

³¹ H.R. 4954: *SAFE Port Act*. Congressional Research Service Summary. <http://www.govtrack.us/congress/bills/110/hr4954?bill=h109-4954&tab=summary> Accessed January 31, 2010.

| | |
|------|--|
| | <ul style="list-style-type: none"> ▪ Multi-Year Funding: Allows funding for multi-year port security projects; ▪ Port Security Training Program: Requires the establishment of a Port Security Training Program to assist facilities to submit a plan to prevent, prepare for, respond to, mitigate against, and recover from acts of terrorism, natural disasters, and other emergencies; ▪ Full Scale Exercises: Requires high risk port facilities to conduct, at least once every two years, live or full-scale exercises to test and evaluate federal, state, and local capabilities to respond to and recover from threats at commercial seaports; ▪ Radiation Scanning: Requires, not later than December 31, 2007, all containers entering high volume U.S. ports by vessel to be scanned for radiation; ▪ Random Inspections / Searches: Requires the DHS Secretary to: <ol style="list-style-type: none"> 1. Ferry Inspections: Develop a plan for the inspection of car ferries bound for a U.S. seaport; 2. Container Searches: Develop and implement a plan for random searches of shipping containers; 3. Port Truck Driver Threat Assessment: Implement a threat assessment screening for all port truck drivers with access to secure areas of a port; and 4. U.S. Virgin Islands (USVI) Border Patrol Unit: Establish a border patrol unit for USVI and report to Congress on the schedule for establishing such unit. ▪ CSI Expansion: Directs the DHS Secretary to establish and implement a CSI program to identify and examine or search maritime containers that pose a security risk <i>before loading in a foreign port for shipment to the United States</i>. Among the new initiatives are: <ol style="list-style-type: none"> 1. Do Not Load Orders: Requires issuance of a "do not load" order to prevent onloading cargo at port designated under CSI that has been identified as high risk; 2. Effectiveness Reports: Requires the DHS Secretary to report to Congress on the effectiveness (and need for improvements) of the CSI by September 30, 2007, and by September 30, 2010; and 3. Appropriations: Authorizes appropriations for FY2008-FY2010 to CBP to carry out the CSI. ▪ C-TPAT Expansion: Authorizes the DHS Secretary, acting through the Commissioner of CBP, to establish C-TPAT, as a voluntary government-private sector program to strengthen the security of the international supply chain and U.S. border security, and to facilitate the movement of secure cargo. Requires the DHS Secretary to review the minimum security requirements of C-TPAT at least once a year; ▪ Cargo Container Screening: Requires the DHS Secretary to: (1) ensure that all incoming cargo containers are screened to identify high-risk containers and that all high-risk containers are scanned or searched; and (2) report to Congress on the status of full-scale implementation of integrated scanning systems for cargo containers; ▪ Reassessment of Ports' Antiterrorism Efforts: Requires the DHS Secretary to reassess the effectiveness of antiterrorism measures maintained at ports not less than once every three years; ▪ Empty Container Security: Directs the DHS Secretary to conduct a one-year pilot program to improve the security of empty containers at U.S. seaports; ▪ Supply Chain Risk Information Gathering: Requires the DHS Secretary to develop a system to collect risk information related to the supply chain with private sector entities; and ▪ Office of Cargo Security: Amends the Homeland Security Act of 2002 to establish, within DHS, an Office of Cargo Security Policy to coordinate all DHS policies relating to cargo security and to consult with stakeholders and coordinate with other federal agencies in establishing standards and regulations and to promote best practices. |
| 2006 | House Resolution 789: Sets forth the rule for consideration of the bill (H.R. 4954) to improve maritime and cargo security through enhanced layered defenses. On May 3, 2006, this resolution passed in the House of Representatives by roll call vote. |
| 2006 | Maritime Infrastructure Recovery Plan (MIRP): The MIRP is one of eight plans supporting the National Strategy for Maritime Security. It was developed in collaboration with public- and private- |

| | |
|------|---|
| | <p>sector stakeholders, as directed by National Security Presidential Directive-41/Homeland Security Presidential Directive-13 (HSPD-13). Its development was also coordinated with other supporting plans, especially the Maritime Transportation System Security Recommendations and the Maritime Commerce Security Plan because of their importance to the secure flow of commerce.</p> <p>In addition to being an integral part of the HSPD-13 plans, the strategic guidance in the MIRP is reflected in the provisions of the National Maritime Security Plan (NMSP). The NMSP is a Maritime Transportation Security Act (MTSA) plan that addresses the restoration of domestic cargo flow following a security incident that occurs under, in, on, or adjacent to waters subject to the jurisdiction of the United States.</p> <p>The Maritime Infrastructure Recovery Plan, the Maritime Commerce Security Plan, and the Maritime Transportation System Security Plan were developed in close coordination under the National Strategy for Maritime Security. The Maritime Commerce Security Plan contains recommendations to promote international maritime supply chain security and the Maritime Transportation System Security Plan addresses security of MTS as a system, including vessels, facilities, and ports. Both support the recovery of maritime capabilities. Since the MIRP provides recovery management procedures for decision makers at various levels, the procedures are general in nature to provide flexibility for recovery management. With over 2,100 possible threat scenarios in hundreds of ports, the variables affecting MTS recovery are too myriad to provide detailed procedures.</p> <p>Nevertheless, the procedures place emphasis on the importance of intelligence gathering and the use of risk management principles to make the decision-making considerations pertinent to any security-incident scenario.</p> |
| 2007 | <p>National Preparedness Guidelines: The DHS Port Security Grant Program requires ports receiving grant funds to align with and support the National Preparedness Guidelines. The <i>Guidelines</i> are umbrella documents that collate many plans, strategies, and systems into an overarching framework, the National Preparedness System. The <i>Guidelines</i> adopt an all-hazards approach to preparedness. An all-hazards approach addresses capabilities-based preparedness to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies. The <i>Guidelines</i> address preparedness for all homeland security mission areas: prevention, protection, response, and recovery.</p> |
| 2007 | <p>Strategy to Enhance International Supply Chain Security: The SafePort Act requires that the Secretary of DHS – in consultation with appropriate federal, state, local, and tribal government agencies, the private sector, and the international community – develop and implement a strategic plan to enhance the security of the international supply chain. The Strategy to Enhance International Supply Chain Security establishes the overarching framework for the secure flow of cargo through the supply chain and builds on existing national strategies, plans specific to individual segments of the supply chain or transportation system, and numerous programs and tactical plans developed and implemented by appropriate DHS components and agencies. Specifically, it follows the flow of cargo throughout the chain – from point of origin to final destination. In addition, It provides the overall strategic structure in which U.S. cargo security programs and efforts operate and clarify how those programs harmonize with similar international programs, such as the World Customs Organization's (WCO) "Framework of Standards to Secure and Facilitate Global Trade."</p> |
| 2007 | <p>Secure Freight Initiative (SFI): DHS and the Department of Energy (DOE) implemented the first phase of SFI, in an effort to build upon existing port security measures by enhancing the federal government's ability to scan containers for nuclear and radiological materials overseas and to better assess the risk of inbound containers. The initial phase of SFI involved the deployment of a combination of existing technology and proven nuclear detection devices to six foreign ports.</p> <p>DHS has made progress in enhancing security in the maritime sector, but key challenges remain. For example, as part of a statutory requirement to scan 100 percent of U.S.-bound container cargo by July 2012, CBP has implemented SFI at select foreign ports. However, CBP does not have a plan for fully implementing the 100 percent scanning requirement by July 2012 because it questions the feasibility. It should be noted however that CBP has not performed a feasibility analysis of the</p> |

| | |
|------|--|
| | requirement. ³² As of October 2009, SFI has been operational at five of these initial seven seaports. ³³ |
| 2007 | <p>NVIC 03-07 Guidance for the Implementation of the TWIC Program in the Maritime Sector: NVIC 03-07 provides guidance on implementation of the TWIC rule which made major changes to 33 CFR Chapter I Subchapter H, 46 CFR Chapter I Subchapter B, and 49 CFR Chapter XII Subchapter D. The TWIC will satisfy the requirement for a biometric credential as mandated by 46 U.S.C. § 70105, which was enacted by the Maritime Transportation Security Act of 2002 (MTSA) and then amended by the Security and Accountability For Every (SAFE) Port Act of 2006.</p> <p>The information in this NVIC details the enrollment and issuance process, provides guidance for successful execution of compliance requirements, provides clarification of the regulations found, and includes a detailed discussion of the actions required by those regulations, with examples, to increase understanding and promote nationwide consistency. The guidelines are intended to help industry comply with the new regulations and COTPs to implement the TWIC program.³⁴</p> <p>TSA, U.S. Coast Guard, and the maritime industry took a number of steps to enroll over 93 percent of the estimated 1.2 million users in the TWIC program (designed to help control access to maritime vessels and facilities) by the April 15, 2009 compliance deadline, but they experienced challenges resulting in delays and in ensuring the successful execution of the TWIC pilot. While DHS and the U.S. Coast Guard have developed a strategy and programs to reduce the risks posed by small vessels, they face ongoing resource and technology challenges in tracking small vessels and preventing attacks by such vessels.³⁵</p> |
| 2008 | <p>NVIC 04-03 Change 3: This change to NVIC 04-03 provides guidance on the acceptable documentary evidence to show that an individual serving as a VSO has met the qualification requirements in 33 CFR 104.215 and the training requirements in the ISPS Code.</p> |
| 2008 | <p>NVIC 09-02 Change 3 Guidelines for Development of Area Maritime Security Committees and Area Maritime Security Plans Required for U.S. Ports: The purpose of this Circular is to accomplish the following:</p> <ol style="list-style-type: none"> 1. AMSCs & Plans: Provide guidance to field commanders on the development and maintenance of AMSCs and Plans; 2. COTP Responsibilities: Provide guidance on the responsibilities of the COTP acting as the Federal Maritime Security Coordinator (FMSC); 3. Security Plan Template: Provide a common template for AMS Plans; 4. Shared Responsibilities: Address port security issues that are the shared responsibility of the port stakeholders and AMSCs; and 5. Unify Efforts: Promote unity of effort among all stakeholders with maritime security interests at the port level. |
| 2009 | <p>NVIC 03-03 Change 2: NVIC 03-03, Change 2 provides implementation guidance for the regulations mandated by the MTSA of 2002 for facilities. This document also introduces the process of submitting security plans and security plan amendments by way of HOMEPOR (U.S. Coast Guard online portal), information regarding the new TWIC rule and its applicability to regulated facilities and requirements of the SafePort Act, including scheduled and non-scheduled facility inspections.</p> |
| 2009 | <p>National Infrastructure Protection Plan (NIPP): NIPP provides the unifying structure for the integration of a wide range of efforts for the enhanced protection and resiliency of the nation's critical infrastructures and key resources (CIKR) into a single national program. The 2009 NIPP replaces the</p> |

³² GAO-10-106, DHS's Progress and Challenges in Key Areas of Maritime, Aviation, and Cybersecurity (2009).

<http://www.gao.gov/new.items/d10106.pdf>. Accessed January 31, 2009.

³³ GAO-10-106, P. 5.

³⁴ The Florida legislature through its July 1, 2009 revisions to FS 311.12 incorporated U.S. Coast Guard guidance set forth in NVIC 03-07, thus making it Florida law.

³⁵ GAO-10-106, P. 1.

| | |
|------|--|
| | 2006 version and reflects changes and updates to program elements and concepts. It captures the evolution and maturation of the processes and programs first outlined in 2006 without changing the underlying policies. The revised NIPP integrates the concepts of resiliency and protection, and broadens the focus of NIPP-related programs and activities to an all-hazards environment. |
| 2010 | <p>Port Security Grant Program (PSGP): PSGP guidance requires that a port area's planning processes align with and support local Area Maritime Security Plans (AMSP) and the National Preparedness Guidelines, as well as incorporate guidance contained in the following:</p> <ul style="list-style-type: none"> ▪ The National Strategy for Maritime Security (2005); ▪ The Maritime Transportation System Security Plan (2005); ▪ The Maritime Infrastructure Recovery Plan (2006); ▪ The International Strategy to Enhance Supply Chain Security (2007); and ▪ The National Infrastructure Protection Plan (2009). |

5.0 Aviation and Maritime Federal Regulations Comparison

5.1 Introduction

The aviation and maritime industries are active all over the world. Aviation air space covers the entire globe while ocean waters cover more than two-thirds of the earth's surface. Protecting these areas from attacks requires the U.S. to provide a layered security system to protect from terrorist groups, hostile nations and any criminals that would commit acts against the U.S., its people and infrastructure. The ability to achieve maritime and aviation security is contingent upon this layered security system that integrates the capabilities of governments and commercial interests throughout the world.

5.2 Layered Security

The U.S. has prioritized the prevention of terrorist attacks, and criminal and hostile acts from occurring. This requires shared responsibilities and costs, thus creating many independent yet interlocking layers of security. The layers include federal, state and local governments, each playing a key role in the multi-layered security system. These agencies are responsible for establishing and enforcing regulations, policies and procedures, identifying threats and appropriate countermeasures, and defining and mitigating risks and vulnerabilities at airports and seaports facilities.

Among the layers of security are:

- **Security Plans:** Aviation and maritime security plans direct a risk-based approach to developing and implementing measures (government regulations/state regulations) to reduce vulnerabilities within the aviation and maritime security systems at airport terminals and seaport facilities;
- **Enhanced Regulations:** Both aviation and maritime have implemented comprehensive enhancements to security measures (government regulations/state requirements) to strengthen aviation-maritime security in a post 9/11 environment; and
- **Physical Protection:** Physical protection is a fundamental layer of security. Both the aviation and maritime sectors established a scalable and flexible security system. This was created to reduce vulnerabilities in both sectors.

Threat Alert System

The U.S. Coast Guard has a three-tiered color-coded system of Maritime Security (MARSEC) levels consistent with the Department of Homeland Security's Homeland Advisory System (HSAS). MARSEC levels are designed to provide a means to easily communicate pre-planned *scalable* responses to increase threat levels.

MARSEC levels reflect the prevailing threat environment to the maritime element of the national transportation system, including ports, vessels, facilities and critical assets and infrastructures located on or adjacent to waters subject to the jurisdiction of the U.S.

HSAS has a five-tiered system for aviation security. It is a color-coded terrorism threat advisory scale. The different levels trigger specific actions by federal agencies and state

and local governments and they affect the level of security at airports and other public facilities.

5.3 Department of Homeland Security Alignment

MARSEC levels are aligned with HSAS – as established by Homeland Security Presidential Directive 3 – and Table 101.205, titled "Relation between HSAS and MARSEC Levels" below shows this alignment.

Table 101.205—Relation between HSAS and MARSEC Levels

| Homeland security advisory system (HSAS) threat condition Aviation | Equivalent maritime security (MARSEC) level |
|---|--|
| Low: Green | MARSEC Level 1. Green, Blue, Yellow |
| Guarded: Blue | |
| Elevated: Yellow | |
| High: Orange | MARSEC Level 2. Orange |
| Severe: Red | MARSEC Level 3. Red |

[USCG–2003–14792, 68 FR 39278, July 1, 2003, as amended at 68 FR 60472, Oct. 22, 2003]

Both the aviation and maritime industries adhere to a multi-layered security alert system. Any one of the current or recommended measures in the layered security system can potentially be compromised but together greatly enhance security. The U.S. has addressed, enhanced and further strengthened all major layers and systems critical to the risk reduction in security. Layered security is not static, but deters attack by continually evolving through calculated improvements.

Listed below are five broad strategic actions that together strengthen U.S. security:

- Maximizing domain awareness;
- Deploying layered security;
- Promoting a safe-secure aviation-maritime transportation system;
- Enhancing international cooperation; and
- Assuring continuity for both aviation-maritime.

The implementation of a multi-layered system at both airports and seaports requires the cooperation of federal departments and agencies, and state and local entities. Furthermore, with foreign partners, this cooperation is essential to further enhance the strength of each measure pursued.

Significant enhancements have been made in the ability to screen persons working in both the aviation and maritime industries. Airport operators require criminal history record checks (CHRC) for all employees, consultants or any persons employed in the airport industry who require unescorted access to restricted areas. Maritime operators require the

Transportation Worker Identification Credential (TWIC) for commercial drivers, dock facility workers and all other persons who may require unescorted access to restricted areas.

5.4 Analysis

This study involved a compilation and review of applicable Aviation Security information from federal, state of Florida, and other local governmental regulatory agency sources. The state of Florida has not implemented regulatory oversight in relation to general or commercial aviation security above and beyond federal regulations. In Florida, security or law enforcement oversight is regulated by the U.S. Department of Transportation / Federal Aviation Administration, while local authorities serve as the enforcement arm. Local law enforcement is generally used and empowered under federal guidelines and laws to enforce criminal and civil actions in general and commercial aviation facilities. While some countries enforce uniform protection at all of their airports, the U.S. controls protection at the state or local level. Primary personnel vary and can include:

- A police force hired and dedicated to the airport;
- A branch (substation) of the local police department stationed at the airport; and
- Members of the local police department assigned to the airport as their normal patrol area.

In the state of Florida, both seaports and airports follow a security agenda that mirrors each other. Security agendas, at first glance, may appear to slightly differ, however, the operational process concerning maritime and aviation security is similar. It involves the implementation of comprehensive layered security measures to enhance the existing security measures. This creates layers of security in each area of the maritime and aviation transportation system.

To better illustrate and compare seaport and airport state requirements and federal regulations, Section 5.5 is provided for reference.

Note: Due to the extensive number of U.S. federal regulations and state of Florida standards for the maritime and aviation industries, an abbreviated comparison is provided to illustrate the most significant areas of concern.

Page Left Blank Intentionally

5.5 Seaport/Airport Comparison

| Code of Federal Regulations | Seaports | Airports |
|---|---|--|
| <p>105.400 Facility Security Plan (FSP) and Security Program for Airports</p> | <p>Facility Security Officer (FSO) must ensure an FSP is developed and implemented for each facility for which he/she designates as the FSO; the FSO must be identified by name and position, and provide 24 hour contact; the FSP must be written in English and must address vulnerabilities, describe security measures for each MARSEC level and be approved by COTP; Written or electronic sensitive security info must be protected..</p> | <p>Security Program 1544.103: The general requirements for each security program must: Provide safety of persons and property traveling on flights provided by the aircraft operator against acts of criminal violence and air piracy, and the introduction of explosives, incendiaries, or weapons aboard an aircraft; Be in writing and signed by the aircraft operator or any person delegated authority in this matter; Be approved by TSA; Each aircraft operator must have a security program; Maintain the original copy of the security program at its corporate office; Have copies of the program at each airport served; Per chapter 1520, the security program must only shared with authorized persons on a need-to-know basis; and the security program must include as specified for that aircraft operator in 1544.101 through 1544.237 regulations.</p> |

| Code of Federal Regulations | Seaports | Airports |
|--|--|---|
| <p>105.405 Format and Content of Facility Security Plan (FSP) and Airport Security Program</p> | <p>Submit one copy of their FSP for review and approval to the cognizant COTP and a letter certifying that the FSP meets applicable requirements of this part; or if intending to operate under an Approved Security Program, a letter signed by the facility owner or operator stating which approved alternative security program the owner or operator intends to use.</p> <p>Owners or operators of facilities not in service on or before December 31, 2003, must comply with the requirements in paragraph (a) of this section 60 days prior to beginning operations or by December 31, 2003, whichever is later. The cognizant COTP will examine each submission for compliance with this part and either: (1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions; (2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or (3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.</p> <p>An FSP may be submitted and approved to cover more than one facility where they share similarities in design and operations, if authorized and approved by each cognizant COTP.</p> | <p>On November 16, 2001, the Aviation and Transportation Security Act (ATSA) was enacted, creating the Transportation Security Administration (TSA) and transferring aviation security functions from the FAA to the TSA. Section 132(a) of ATSA required the Under Secretary of Transportation for Security to "implement a security program for charter air carriers... with a maximum certificated takeoff weight of 12,500 pounds or more." On February 22, 2002, a final rule was published in the Federal Register that required that "certain aircraft operators using aircraft with a maximum certificated takeoff weight of 12,500 pounds or more carry out security measures." The rule also required that "certain aircraft operators conduct criminal history records checks on their flight crew members, and restrict access to the flight deck." The "certain aircraft operators" were defined as those conducting operations "in scheduled or charter service, carrying passengers or cargo or both..." The program that outlines the security measures and requirements for these operators is known as the Twelve-Five Standard Security program (TFSSP).</p> |

| Code of Federal Regulations | Seaports | Airports |
|---|--|---|
| <p>105.410 Submission and approval for security plans for Seaports and Airports</p> | <p>Submit one copy of their FSP for review and approval to the cognizant COTP and a letter certifying that the FSP meets applicable requirements of this part; or if intending to operate under an Approved Security Program, a letter signed by the facility owner or operator stating which approved alternative security program the owner or operator intends to use.</p> <p>Owners or operators of facilities not in service on or before December 31, 2003, must comply with the requirements in paragraph (a) of this section 60 days prior to beginning operations or by December 31, 2003, whichever is later. The cognizant COTP will examine each submission for compliance with this part and either: (1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions; (2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or (3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.</p> <p>An FSP may be submitted and approved to cover more than one facility where they share similarities in design and operations, if authorized and approved by each cognizant COTP.</p> | <p>On November 16, 2001, the Aviation and Transportation Security Act (ATSA) was enacted, creating the Transportation Security Administration (TSA) and transferring aviation security functions from the FAA to the TSA. Section 132(a) of ATSA required the Under Secretary of Transportation for Security to "implement a security program for charter air carriers... with a maximum certificated takeoff weight of 12,500 pounds or more." On February 22, 2002, a final rule was published in the Federal Register that required that "certain aircraft operators using aircraft with a maximum certificated takeoff weight of 12,500 pounds or more carry out security measures." The rule also required that "certain aircraft operators conduct criminal history records checks on their flight crew members, and restrict access to the flight deck." The "certain aircraft operators" were defined as those conducting operations "in scheduled or charter service, carrying passengers or cargo or both..." The program that outlines the security measures and requirements for these operators is known as the Twelve-Five Standard Security program (TFSSP).</p> |
| <p>105.105 workers identification, records checks and credentials for Seaports/Airports</p> | <p>Transportation Worker Identification Credential (TWIC) is required at all U.S. seaports.</p> | <p>Criminal History Records Check (CHRC) is required for all airports.</p> |

| Code of Federal Regulations | Seaports | Airports |
|--|---|---|
| <p>Terminal/Facility for Maritime 105.106 and Airport Terminal 1544/1546</p> | <p>Areas defined as any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the U.S. and used operated, or maintained by a public private entity, including and contiguous or adjoining property under common ownership or operation.</p> | <p>Airport means any public-use airport, including heliports, as defined in 49 U.S.C. 47102, including public airports and privately owned airports used for public purposes a reliever airport (at least 2,500 passengers a year) and receives scheduled passenger aircraft service. A portion of an airport, specified in the Airport Security Program in which certain security measures specified in Title 49 of the Code of Federal Regulations are carried out. This area is where aircraft operators and foreign air carriers that have a security program under 49 CFR part 1544 or part 1546 enplane and deplane passengers and sort and load luggage and any adjacent areas that are not separated by adequate security systems, measures, or procedures.</p> |
| <p>105.145 Maritime Security Three Tiered Levels and Aviation 5 Tiered HSAS Levels</p> | <p>Three-tiered system of MARSEC levels consistent with the HSAS. Owner/operator must comply with all instructions contained.</p> <p>MARSEC levels:</p> <p>Green, Blue, Yellow: Low/Guarded/Elevated Orange: High Red: Severe</p> | <p>5 tiered system of Aviation Security Advisory System (HSAS) In the U.S. the HSAS is a color-coded terrorism threat advisory scale. The different levels trigger specific actions by federal agencies and state and local governments, and the affect the level of security at some airports and seaports and other public facilities.</p> <p>Low Green: low risk Guarded Blue: general risk Elevated yellow: significant risk High Orange: high risk Severe: Red severe risk</p> |

| Code of Federal Regulations | Seaports | Airports |
|--|--|---|
| 105.200 Owner/Operator Seaport Facility and Airport Operator | Defined as any person or entity that maintains operational control over any facility, vessel, or Offshore Coastal Shelf (OCS) facility and is subject to the requirements of this subchapter maintenance of the FSP and liaison with the COTP. | Airport Operator means a person that operates an airport serving an aircraft operator or a foreign air carrier required to have a security program under part 1544 or 1546 of this chapter. Each airport operator is required to have a security program and must establish at least one secure area. |
| 105.205 Maritime Facility Security Officer and 1542.3 Airport Security Coordinator | Defined as the person designated as responsible for the development, implementation, revision and maintenance of the facility security plan and for liaison with the COTP, company and Vessel Security Officer (VSO) must have knowledge of FSP, training relative to the terminal, security operations relevant to international laws, codes, responsible for all security aspects and requirements. FSO must notify vessel of any security incident and must also be available 24-7. | Each airport operator must designate one or more (ASC)'s in its security plan. ASC serves as operator's primary and immediate contact for security related activities and communication with the TSA and must also be available 24-7. Must complete all training as specified in its security program. Airport operator must maintain ASC training doc's until at least 180 days after individuals withdraw from ASC position. Each aircraft operator must designate and use an Aircraft Operator Security Coordinator (AOSC). The AOSC and any alternates must be appointed at the corporate level and must serve as the aircrafts primary contact for security related activities and communications with TSA as set forth in the security program. Either the AOSC or an alternate must be available 24-7 basis. Ground Security Coordinator is responsible for carrying out ground security duties specified in the security program. In-flight security coordinator is the on board pilot in command he performs the duties specified in the aircraft operator's security program. |

| Code of Federal Regulations | Seaports | Airports |
|--|---|--|
| 105.210 Seaport Facility Personnel with security duties and Airport facility security personnel with security duties | Must have TWIC, training in appropriate security areas and security related common knowledge of: threats, patterns, devices, substances, crowd management, and security equipment. All other facility personnel must have knowledge through training of relevant security provisions of the FSP. | Must have TWIC, training in appropriate security areas and security related common knowledge of: threats, patterns, devices substances, crowd management, also knowledge of security equipment. Each airport operator must ensure that individuals performing security related functions for the airport operator are briefed on the provisions of this part. Security personnel need to know the information and security circulars and directives in order to perform their security duties. |
| Seaport 105.255 and Airport 1540.107 (submission to screening) | No individual may enter a sterile area or board a vessel without submitting to the screening and inspection of his or her person, vehicles and accessible property in accordance with the procedures being applied to control access to that area or vessel under this chapter. Individuals being screened must produce identification, must have reservations for a covered cruise and must make a request to enter the sterile area. Excluding government-owned vehicles on official business when government officials produce identification credentials. | No individual may enter a sterile area or board an aircraft without submitting to the screening and inspection of his or her person and accessible property in accordance with the procedures being applied to control access to that area or aircraft under chapter 1540.107. Individuals being screened must produce identification, must have reservation for a covered flight and must make a request to enter the sterile area. |

| Code of Federal Regulations | Seaports | Airports |
|--|--|--|
| 105.220 Drills and Exercise requirements for Seaport and Airport | Drills and exercises must test proficiency of facility personnel in assigned security duties at all MARSEC levels and must enable the FSO to identify any related security deficiencies that need to be addressed. Drills and exercises must test individual elements of the FSP, such as unauthorized entry to restricted areas, alarm response notification to law enforcement, etc.. | Drills and exercises must test proficiency of airport security personnel in assigned security duties at all HSAS threat levels. Must enable the aviation security coordinators to identify any related security deficiencies that need to be addressed. Drills and exercises must test individual elements of the Airport Security Program, such as unauthorized entry to sterile restricted areas alarm response, notification to law enforcement on unauthorized entry to restricted areas, etc. |
| 105.225 Facility Record Keeping requirements for Seaports and Airports | Facility personnel responsible for security duties must maintain a TWIC, and must have knowledge, through training or equivalent job experience, in the following, as appropriate:(a) knowledge of current security threats and patterns;(b) recognition and detection of dangerous substances and devices;(c) recognition of characteristics and behavioral patterns of persons who are likely to threaten security;(d) techniques used to circumvent security measures;(e) crowd management and control techniques;(f) security related communications;(g) knowledge of emergency procedures and contingency plans;(h) operation of security equipment and systems;(i) testing, calibration, and maintenance of security equipment and systems;(j) inspection, control, and monitoring techniques;(k) relevant provisions of the Facility Security Plan (FSP);(l) methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores;(m) the meaning and the consequential requirements of the different MARSEC Levels; and(n) be familiar with all relevant aspects of the TWIC program and how to carry them out. | Each validation firm must maintain records demonstrating compliance with all statutes, regulations, directives, orders, and security programs that apply to operations as a validation firm, including the records listed below. Each validation firm must retain the following records for 180 days after the individual is no longer employed by the validation firm or is no longer acting as the firm's agent. Airport must maintain: (1) records of all training and instruction given to each individual under the requirements of this subpart; (2) records demonstrating that the validation firm has complied with the security threat assessment provisions of § 1522.121; and (3) records about the qualifications of validators it uses to conduct assessments under this subpart. |

| Code of Federal Regulations | Seaports | Airports |
|--|--|---|
| <p>105.215 Seaport Training and 154.213 Airport Training</p> | <p>Facility personnel responsible for security duties must maintain a TWIC, and must have knowledge, through training or equivalent job experience, in the following, as appropriate:(a) knowledge of current security threats and patterns;(b) recognition and detection of dangerous substances and devices; (c) recognition of characteristics and behavioral patterns of persons who are likely to threaten security;(d) techniques used to circumvent security measures;(e) crowd management and control techniques;(f) security related communications;(g) knowledge of emergency procedures and contingency plans;(h) operation of security equipment and systems;(i) testing, calibration, and maintenance of security equipment and systems;(j) inspection, control, and monitoring techniques;(k) relevant provisions of the FSP;(l) methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores;(m) meaning and the consequential requirements of the different MARSEC levels; and (n) be familiar with all relevant aspects of the TWIC program and how to carry them out.</p> | <p>Each airport operator must ensure that individuals performing security-related functions for the airport operator are briefed on the provisions of this part, Security Directives, and Information Circulars, and the security program, to the extent that such individuals need to know in order to perform their duties. An airport operator may not authorize any individual unescorted access to the secured area or SIDA, except as provided in §1542.5, unless that individual has successfully completed training in accordance with TSA-approved curriculum specified in the security program. This curriculum must detail the methods of instruction, provide attendees with an opportunity to ask questions, and include at least the following topics: (1) unescorted access authority of the individual to enter and be present in various areas of the airport;(2) control, use, and display of airport-approved access and identification media;(3) escort and challenge procedures and the law enforcement support for these procedures;(4) security responsibilities as specified in §1540.105;(5) restrictions on divulging sensitive security information as described in part 1520 of this chapter; and (6) any other topics specified in the security program.</p> |

| Code of Federal Regulations | Seaports | Airports |
|---|--|---|
| <p>105.230 Maritime and 1540.205 Aviation Security coordination and implementation of threat levels</p> | <p>Facility owner/operator must ensure the facility operates in compliance with security requirements in this part for the MARSEC level in effect for the port. When notified of a MARSEC threat level increase, owner/operator must ensure that vessels moored to the facility and vessels scheduled to arrive at the facility within 96 hours of the MARSEC level change are notified of the new MARSEC level and the Declaration of Security (DoS) is revised and necessary. Facility must comply with the required additional security measures within 12 hours and reports compliance or non-compliance to the COTP.</p> <p>At MARSEC level 2 and 3 FSO must inform personnel about identified threats, emphasize reporting procedures and stress the need for increased vigilance. Owner/operator not in compliance with requirements in this section must inform the COTP and obtain approval prior interfacing with a vessel or continuing operations.</p> <p>At MARSEC level 3, in addition to the requirements in this part, a facility owner/operator may be required to implement additional measures pursuant to 33CFR part 6, 160 or 165 as appropriate which may include but not limited to waterborne patrol, armed security to control access to the facility and to deter, to the maximum extent practical, a transportation security incident and examination of piers, wharves and similar structures at the facility for the presence of dangerous substances or devices underwater or other threats.</p> | <p>After approval of the security program, each airport operator must notify TSA when changes have occurred to: measures, training, area descriptions, or staffing, described in the security program; operations of an aircraft operator or foreign air carrier that would require modifications to the security program as required; or layout or physical structure of any area under the control of the airport operator, airport tenant, aircraft operator, or foreign air carrier used to support the screening process, access, presence, or movement control functions required under part 1542, 1544, or 1546 of this chapter.</p> <p>Each airport operator must notify TSA no more than 6 hours after the discovery of any change in condition described above, or within the time specified in its security program. The airport operator must inform TSA of each interim measure being taken to maintain adequate security until an appropriate amendment to the security program is approved. Each interim measure must be acceptable to TSA.</p> <p>For changed conditions expected to be less than 60 days duration, each airport operator must forward the required information in writing to TSA within 72 hours of the original notification of the change condition(s). TSA will notify the airport operator of the disposition of the notification in writing. If approved by TSA, this written notification becomes a part of the airport security program for the duration of the changed condition(s).</p> <p>For changed conditions expected to be 60 days or more duration, each airport operator must forward the information required in the form of a proposed amendment to the airport operator's security program. The request for an amendment must be made within 30 days of the discovery of the changed condition(s).</p> |

| Code of Federal Regulations | Seaports | Airports |
|--|--|---|
| 105.235 Communications for Seaport and Airport | <p>The FSO must have a means to effectively notify facility personnel of changes in security conditions at the facility. At each active facility access point, the facility must provide a means of contacting police, security control, or an emergency operations center, by telephone, cellular phones, and/or portable radios or other equivalent means. Security systems and equipment must be in good working condition/order and inspected tested, calibrated and maintained according to manufactured recommendations. Facility communications systems must have a backup means for both internal and external communications.</p> | <p>The Airport Security Coordinator (ASC) must have a means to effectively notify airport (TSA) personnel of changes in security conditions at the facility. At each active airport access point provide a means of contacting police, security control, or an emergency operations center, by telephone, cellular phones, and/or portable radios or other equivalent means security systems and equipment must be in good working condition/order and inspected tested, calibrated and maintained according to manufactured recommendations. No aircraft operator may use such system in a manner contrary to its security program. Airport communications systems must have a backup means for both internal and external communications.</p> |
| 105.250 Security Systems and Equipment Maintenance for Seaports and Airports | <p>Security systems and equipment must be in good working condition/order and inspected tested, calibrated and maintained according to manufactured recommendations.</p> | <p>Security systems and equipment must be in good working condition/order and inspected tested, calibrated and maintained according to manufactured recommendations No aircraft operator may use such system in a manner contrary to its security program.</p> |

| Code of Federal Regulations | Seaports | Airports |
|--|--|--|
| <p>105.255 Security measures for access control at Seaports and Airports</p> | <p>The owner/operator must ensure the implementation of security measures to deter, secure, control and prevent access to the facility and deter dangerous substances and devices including any device to destroy persons, vessels, facilities, or ports.</p> <p>The owner/operator must control access to the facility and prevent individuals from entering an area of the facility that is designated as a secure area unless they have a TWIC or are authorized to be in the area.</p> <p>Restricted areas must include, as appropriate: shore areas immediately adjacent to each vessel moored at the facility; cargo areas with documentation; areas containing security and surveillance equipment; lighting system controls; areas containing critical facility infrastructure; water supplies; telecommunications; electrical systems; access points for ventilation; processing areas and control rooms; restricted areas for vehicles and personnel; areas designated for loading/unloading; and storage for cargo and stores (See MARSEC levels for increased additional security levels in restricted areas).</p> | <p>Except as provided in paragraph (b) of this section, the measures for controlling entry to the secured area required under §1542.201(b)(1) must: (1) ensure that only those individuals authorized to have unescorted access to the secured area are able to gain entry;(2) ensure that an individual is immediately denied entry to a secured area when that person's access authority for that area is withdrawn; and (3) provide a means to differentiate between individuals authorized to have access to an entire secured area and individuals authorized access to only a particular portion of a secured area.</p> <p>TSA may approve an amendment to a security program that provides alternative measures that provide an overall level of security equal to that which would be provided by the measures described above.</p> <p>The measures for controlling entry to the Air Operations Area (AOA) required under §1542.203(b)(1) must incorporate accountability procedures to maintain their integrity.</p> <p>An airport operator may issue a second access medium to an individual who has unescorted access to secured areas or the AOA, but is temporarily not in possession of the original access medium, if the airport operator follows measures and procedures in the security program that:(1) verifies the authorization of the individual to have unescorted access to secured areas or AOAs; (2) restricts the time period of entry with the second access medium;(3) retrieves the second access medium when expired;(4) deactivates or invalidates the original access medium until the individual returns the second access medium; and (5) provides that any second access media that is also used as identification media meet the criteria.</p> |

| Code of Federal Regulations | Seaports | Airports |
|---|--|---|
| <p>105.260 Seaport security measures for restricted areas and Airport security measures for restricted areas 1542.207</p> | <p>The facility owner/ operator must ensure restricted areas are designated within the facility. They must also ensure that all restricted areas are clearly marked and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security. The facility owner/operator may also designate the entire facility as a restricted area.</p> <p>Restricted areas must include, as appropriate: shore areas immediately adjacent to each vessel moored at the facility; cargo areas with documentation; areas containing security and surveillance equipment; lighting system controls; areas containing critical facility infrastructure; water supplies; telecommunications; electrical systems; access points for ventilation; processing areas and control rooms; restricted areas for vehicles and personnel; areas designated for loading/unloading; and storage for cargo and stores (See MARSEC levels for increased additional security levels in restricted areas).</p> | <p>The airport operator must ensure restricted areas are designated within the airport. They must also ensure that all restricted areas are clearly marked and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security. Restricted areas include AOAs as a portion of an airport; areas specified in the airport security program, in which security measures specified in this part are carried out. This area includes aircraft movement areas; aircraft parking areas; loading ramps; and safety areas for use by aircraft regulated under 49 CFR part 1544 or 1546, and any adjacent areas (such as general aviation areas) that are not separated by adequate security systems, measures, or procedures. This area does not include the secured area.</p> <p>Security Identification Display Area (SIDA) means a portion of an airport, specified in the airport security program, in which security measures specified in this part are carried out. This area includes the secured area and may include other areas of the airport.</p> |
| | | |

| Code of Federal Regulations | Seaports | Airports |
|--|---|--|
| <p>105.265 Security measures for handling cargo at Seaports and Airports</p> | <p>The facility owner/operator must ensure that security measures relating to cargo handling, some of which may have to be applied in liaison with the vessel, are implemented in order to: deter tampering; prevent cargo that is not meant for carriage from being accepted and stored at the facility without the knowing consent of the facility owner or operator; identify cargo that is approved for loading onto vessels interfacing with the facility; include cargo control procedures at access points to the facility; identify cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up; restrict the entry of cargo to the facility that does not have a confirmed date for loading, as appropriate; ensure the release of cargo only to the carrier specified in the cargo documentation; when there are regular or repeated cargo operations with the same shipper, coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedure; and create, update, and maintain a continuous inventory of all dangerous goods and hazardous substances from receipt to delivery within the facility, giving the location of those dangerous goods and hazardous substances.</p> | <p>Each aircraft operator operating under a full program, a full all-cargo program or a twelve-five program in all-cargo operation must use the procedures, facilities, and equipment described in its security program to prevent or deter the carriage of any unauthorized persons, and any unauthorized cargo or items onboard an aircraft. The cargo reaches a location where an aircraft operator with a full all-cargo program consolidates or inspects it pursuant to security program requirements until the cargo enters an airport Security Identification Display Area (SIDA) or is transferred to another TSA-regulated aircraft operator, foreign air carrier, or indirect air carrier; or an aircraft operator with a full program accepts the cargo until the cargo enters an airport SIDA is removed from the destination airport; or is transferred to another TSA-regulated aircraft operator, foreign air carrier; or indirect air carrier each individual the aircraft operator authorizes to screen cargo or to supervise the screening of cargo under §1544.205 (e) acceptance of cargo only from specified persons.</p> <p>Each aircraft operator operating under a full program or a full all-cargo program may accept cargo to be loaded in the United States for air transportation only from the shipper, an aircraft operator, foreign air carrier, or indirect air carrier operating under a security program under this chapter with a comparable cargo security program, or, in the case of an operator under a full program, from a certified cargo screening facility, as provided in its security program.</p> |

| Code of Federal Regulations | Seaports | Airports |
|---|---|---|
| <p>105.275 Security measures for monitoring Seaports and Airports</p> | <p>The owner/operator must ensure the implementation of security measures in this section and have the capability to continuously monitor, through a combination of lighting, security guards, waterborne patrols, automatic intrusion detection devices, or surveillance equipment as specified in the approved FSP (See MARSEC threat levels for increased additional security levels pertaining to security monitoring).</p> | <p>Each airport operator is required to have a security program under §1542.103(a) and must establish at least one secured area. Each airport operator is required to establish a secured area and must prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into and within the secured area by doing the following: establish and carry out measures for controlling entry to secured areas of the airport in accordance with §1542.207; provide for detection of, and response to, each unauthorized presence or movement in, or attempted entry to, the secured area by an individual whose access is not authorized in accordance with its security program; establish and carry out a personnel identification system described under §1542.211; subject each individual to employment history verification as described in §1542.209 before authorizing unescorted access to a secured area; train each individual before granting unescorted access to the secured area, as required in §1542.213(b); and post signs at secured areas access points and on the perimeters that provide warning of the prohibition against unauthorized entry.</p> |

| Code of Federal Regulations | Seaports | Airports |
|---|---|--|
| <p>105.280 Security Incident Procedures and 1542.303 Airport Security Changes (security directives/information circulars)</p> | <p>For each MARSEC level the facility owner/operator must ensure the FSO and facility security personnel are able to respond to security threats and breaches of security, maintain critical facility and vessel-to-facility interface operations, and evacuate the facility in case of security threats or breaches of security.</p> <p>Security incidents must be reported as required in 101.305 of this subchapter. FSOs must brief all facility personnel on possible threats and need for vigilance, soliciting their assistance in reporting suspicious persons, objects or activities and secure non-critical operations in order to focus response on critical operations.</p> | <p>TSA may issue an Information Circular to notify airport operators of security concerns. When TSA determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against civil aviation, TSA issues a Security Directive setting forth mandatory measures.</p> <p>Each airport operator must comply with each Security Directive issued to the airport operator within the time prescribed in the Security Directive.</p> <p>Each airport operator that receives a Security Directive must, within the time prescribed in the Security Directive, verbally acknowledge receipt of the Security Directive to TSA and specify the method by which the measures in the Security Directive have been implemented or will be implemented, if the Security Directive is not yet effective).</p> <p>In the event that the airport operator is unable to implement the measures in the Security Directive, the airport operator must submit proposed alternative measures and the basis for submitting the alternative measures to TSA for approval. The airport operator must submit the proposed alternative measures within the time prescribed in the Security Directive. The airport operator must implement any alternative measures approved by TSA.</p> <p>Each airport operator that receives a Security Directive may comment on the Security Directive by submitting data, views, or arguments in writing to TSA. TSA may amend the Security Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive.</p> <p>Each airport operator that receives a Security Directive or an Information Circular and each person who receives information from a Security Directive or an Information Circular must restrict the availability of the Security Directive or Information Circular, and information contained in either document, to those persons with an operational need-to-know and refuse to release the Security Directive</p> |

| Code of Federal Regulations | Seaports | Airports |
|--|--|---|
| | | or information circular and information contained in either document to persons with a need to know. |
| <p>105.305 Facility Security Assessment (FSA) and Airport Requirements (on scene survey)</p> | <p>The facility owner/operator must ensure that the following background information if applicable is provided to the person or persons who will conduct the assessment: general layout of the facility; locations of each active and inactive access points to the facility; security duties of facility personnel; security doors barriers and lighting; location of restricted areas; equipment; escape/evacuation; response procedures; cargo spaces; storage spaces; security and safety equipment; protection of passengers and personnel; and threat assessments.</p> | <p>Each valuator must prepare and submit to TSA a written assessment report, in a manner and form prescribed by TSA, within 30 calendar days of completing each assessment. The assessment report must include the following information in addition to any other information otherwise required by TSA: description of the facilities, equipment; systems, processes, and any other information as determined by TSA; the valuator's assessment regarding the facility's compliance with TSA requirements including all elements of the applicable security program; and signed testimony by the individual valuator with responsibility for the assessment that no conflicts of interest existed with regard to the assessment and that the assessment was conducted impartially, professionally, and consistent with the standards set forth by TSA.</p> |

6.0 State and Federal Regulation Evaluation

6.1 Introduction

This section of the report contains a state and federal regulation comparative analysis of the security mechanisms in place to help Florida's commercial seaports to deter, detect, delay, and respond to credible threats to their facilities, operations, and personnel.

Given the unique regulatory environment in Florida, it is important to evaluate how the existing state and federal maritime security laws and regulations support a layered system of protection. The objective of this section of the report is to identify the gaps, overlaps, and conflicts that exist between the current state and federal maritime security regulations. This section will also recommend corrective actions designed to promote and support the alignment of state and federal security standards and practices to create a more secure, functional, and cost-effective operational environment for Florida's commercial maritime community.

It should be noted that the legislative intent, security standards, and performance objectives included in the revised Florida Statute (FS) 311.12 (2009) statute have not yet been implemented. In addition, interviews with security and management personnel at Florida's seaports indicate an overall unawareness of the impact of these changes on the compliance inspection expectations and standards for achievement, especially for those security standards or performance objectives that are subject to "alignment with federal standards and performance measures."

6.2 Recommendations

Identification of Applicable Seaports: The language in FS 311.09 (1) that identifies the 14 specific commercial ports, for which the statute is applicable, should be revoked or amended. In order to effectively align the application of FS 311.12 standards to the same set of commercial seaports, facilities, and activities to which the federal statutes apply, the state regulation should be amended to mirror that shown in U.S. Coast Guard's 33 CFR, part 105.105.

Security Standards: The minimum security standards outlined in the Office of Drug Control (ODC) / Florida Department of Law Enforcement (FDLE)-developed Port Security Standards Compliance Plan (2001) is inconsistent or mutually exclusive with the Legislature's stated intent of aligning the state and federal security standards applied to Florida's commercial seaports. This creates significant conflict in providing a consistent interpretation of security standards and practices for application across Florida's commercial maritime environment. Effective alignment of state and federal standards may best be accomplished by the elimination of the prescriptive standards outlined in the Port Security

Standards Compliance Plan (2001), and the adoption of the more flexible, risk- and performance-based federal standards.

Port / Facility Security Plans: The FS 311.12-required facility security plan lacks of a standardized format and content in contrast to the MTSA-required plan. As a result, Florida's ports maintain Facility Security Plans (FSP) with redundant or conflicting sections to address requirements specific to the respective standards. In some cases, this has resulted in the creation a facility keeping two plans, once compliant with FS 311.12, the other, with the MTSA. Maintaining two plans is not conducive to the effective implementation of security at a seaport. Adoption of the federal guidelines for format and content of FSPs for commercial seaports and their operations will eliminate the conflicts, and greatly enhance the functional alignment of state and federal standards.

Identification of Secured & Restricted Areas: In accordance with directive in FS 311.12 (2009) state and federal definitions of secure and restricted areas will be aligned. In order for the alignment to be effective, all other definitional language used to interpret compliance with the state statute, as incorporated in the Port Security Standards Compliance Plan (2001), will need to be amended or revoked.

Identification of Exempted Areas: The current process for the identification and granting of area exemptions may be expedited by expanding the charter of the Seaport Security Standards Advisory Council (SSSAC) to include this function, and establishing a timeline for the review and adjudication of each port's exemption requests.

ID / Access Control Badges: FS 311.12 (2009) requires that any person seeking unescorted access to secure and restricted areas of a Florida seaport must possess a valid TWIC. This requirement is duplicative of the requirement for issuance and use of ID / Access Control badges which are issued by each Florida port to facilitate access control and accountability of persons entering secure or restrictive areas. Issuance of a Florida port ID / Access Control Badge is still maintained as a standard in the Port Security Standards Compliance Plan (2001), and is issued only after successful completion of an FDLE-conducted criminal background check against state felony standards and payment of a fee. Alignment of state and federal standards may be accomplished by:

- Eliminating or amending the section of the Port Security Standards Compliance Plan (2001) relating to the criteria for issuance and retention of Florida port ID / Access Control Badges;
- Aligning state and federal criminal background investigation standards for disqualification to support the conduct of a single check for issuance of either credential;
- Eliminating the background check and fee requirement for issuance of a Florida port ID / Access Control Badge to persons already in possession of a valid TWIC; or

-
- Establish a mechanism for communicating between state and federal law enforcement agencies responsible for conducting ID eligibility background investigations to facilitate the timely exchange of valid disqualifying information.

Note: Florida port representatives consistently voiced their desire to retain local control over granting unescorted access to their port's secure and restricted areas, which may best be effected through the continued issuance of Florida port ID / Access control Badges. Streamlining the background investigation process, and elimination of additional fees for individuals who have already been issued a valid TWIC will greatly enhance the Florida ports' ability to achieve the intent of the Legislature for alignment of state and federal ID / Access Control standards.

TWIC Possession & Retention: While FS 311.12 (2009) establishes TWIC as the only credential authorized for use by Florida's commercial seaports, Florida's ports are still subject to FDLE compliance audits against the minimum security standards outlined in the Port Security Standards Compliance Plan (2001). Alignment of state and federal requirements for use of TWIC to access a Florida port's secure and restricted areas will require the removal of conflicting standards for background checks, disqualifying criteria, and fee payment. However, the most immediate and effective solution to this conflict is for the Florida Legislature to revoke or void the minimum security standard requirements for ID badges identified in Section 1 of the Port Security Standards Compliance Plan (2001).

Access Eligibility Reporting System (AERS): This is a new requirement for the collection and transmission of information developed as a result of the FDLE criminal background investigations, against disqualification standards based on state felony definitions, for issuance of port ID/Access badges. The security systems and equipment required for the collection, maintenance, and timely transmission of an applicant's access authorization or disqualification is not yet been identified, procured, installed or integrated with state law enforcement criminal data management systems to ensure its effective operation.

If the Legislature's intent of adopting TWIC as the only credential authorized for use to access secure and restricted areas in Florida's ports, and the TWIC is issued based on a federal investigation for qualification or disqualification, then the AERS system seems to be redundant, and is subject to result in the issuance or disqualification of state and federal ID credentials based on conflicting standards.

Access Gates & Gate Houses

Designated Parking: Both state and federal standards limit vehicle access to and parking in secure and restricted areas. State standards mandate that ports use a vehicle pass and / or decal system, which is prescriptive in nature. Alignment of the state and federal practices for this requirement may best be accomplished by eliminating the

prescriptive state standards and by adopting the federal, performance-based standards.

Fencing & Barriers: The intended function of security fencing and barriers is the same in both the state and federal statutes. However, Florida's statute establishes specific, prescriptive materials, construction, and maintenance requirements for fencing and barriers used to delineate the boundaries and support the enforcement of access control for secure and restricted areas. However, the state standards do not take into consideration whether the designated secure or restricted areas, as defined in the *Port Security Standards Compliance Plan* (2001), are consistent with the port's threat and risk profiles and operational requirements.

Current state requirements conflict with the performance-based federal requirements for fencing and barriers, and have resulted in the unnecessary expenditure of limited financial resources by a number of Florida ports to meet the state's prescriptive requirement for areas that would not be identified as "restricted" under the federal standards.

Alignment of state and federal standards for fencing and barriers may be best and most effectively served by legislative repeal or revocation of the prescriptive minimum security standards identified in the *Port Security Standards Compliance Plan* (2001), and the adoption of the federal standards and practices for fencing and barriers.

Lighting: Current requirements for lighting and illumination for areas identified as restricted, as defined in the *Port Security Standards Compliance Plan* (2001), do not take into consideration whether the designated secure or restricted areas – for which the specific lighting and illumination standards are to be applied – are consistent with the port's threat and risk profiles, and operational requirements. In addition, the state's standards are not flexible enough to reasonably accommodate local municipal, state, or federal environmental, anti-light pollution or nuisance ordinances.

Alignment of state and federal standards for lighting and illumination may be most efficiently implemented by legislative repeal or revocation of the prescriptive minimum security standards identified in the *Port Security Standards Compliance Plan* (2001), and the adoption of the federal standards and practices for lighting and illumination.

Security Signage: Requirements and standards for security signage are fairly consistent between state and federal standards. However, effective alignment of current state and federal requirements recommend the modification of the existing state standard for specific security signage language in favor of general guidance as to the information the sign must convey.

Lock & Key Controls: Existing state requirements and standards for lock and key control are not in conflict with federal requirements. No modifications are recommended.

Intrusion Detection & Monitoring Systems: Alignment of the state and federal standards and guidelines for the use of intrusion detection and monitoring systems may best be implemented through the revocation of the prescriptive standards identified in the Port Security Standards Compliance Plan (2001), and the adoption of the more flexible guidelines included in the federal statute.

Security (Planning) Committees: Both state and federal statutes establish committees for the discussion of issues related to the planning and execution of security requirements. The Committee established by the state statute is limited to representatives from port management, security management, and stakeholders of each seaport. The federal statute establishes an Area Maritime Security Committee (AMSC) that is chaired by the U.S. Coast Guard Sector Commander, and includes representatives from the larger maritime, law enforcement, supporting transportation, and supply chain communities within the Sector Commander's geographic area of responsibility.

Each port security committee, and its supporting stakeholder community, is already represented on the AMSC in which they are geographically located. Further alignment action is recommended to limit unnecessary duplication of functions and representations of the participating organizations.

Security Standard Operating Procedures (SOPs): Align state and federal standards in the structure and content of state-mandated Seaport Security Plans (SSP) and the federal FSPs. This will enhance the education, execution, and enforcement of security procedures and practices included in the required SOPs. Adopt 33 CFR 105.405 for the format and content of a consolidated state and federal FSP is recommended.

Law Enforcement Presence: Relax the requirement for the presence of state-certified law enforcement officers to perform seaport security patrols, and recognize the deterrent effect the presence of federal law enforcement officers bring to port security.

Security Guard Force: Current state standards for Class D or G certification of contract security guard force personnel may readily be integrated into the federal training requirements for security personnel with specific security duties.

Certified Seaport Security Officer Detention Authority: This requirement is specific to the state statute, and reinforces the operational relationship between state-certified Seaport Security Officers and federal law enforcement officers at Florida's seaports.

Security Training, Drills & Exercises: Adoption of federal security standards for training and certification of port personnel with and without specific security responsibilities should be used as the basis for compliance with the state training requirements. Additional security training above and beyond the federal standards may be implemented as a means of career development and professionalization.

Maritime Domain Security Awareness Training Program: In order to ensure identification and understanding of credible threats, and the process for determining the threat and developing risk mitigation plans, it is recommended that Florida adapt the U.S. Coast Guard's Maritime Domain Awareness Training standards and practices, rather than dedicating manpower and financial resources to recreating an existing federal program.

Information Security (INFOSEC): State and federal procedures for ensuring the security, handling, and control of Sensitive Security Information (SSI) may best be aligned by adoption and implementation of the requirements outlined in 49 CFR, Part 1520.

Equipment Control: The intent of this requirement is consistent between state and federal statutes.

Cruise Operations Security: The state statutes direct, by reference, compliance with the federal standards for vessel and passenger cruise terminal security. Further action may be needed to effectively align state and federal standards regarding the:

- Alignment of passenger terminal secure and restricted areas;
- Accepted compliance standard for the placement and use of security screening equipment; and
- ID badging and access requirements for cruise terminal employee and vendor personnel.

Waiver from Security Requirements: Both the state and federal regulations have an established process for requesting waivers from security requirements identified in the respective statutes. Due to the lack of connection in the chain of authority for enforcement of state and federal security standards – specifically state and federal waiver review and approval mechanisms – alignment of the state and federal waiver standards is unlikely to be actionable in a timely or effective manner.

SSSAC: The SSSAC membership is over-represented by state government agencies whose knowledge and understanding of the evolving federal and state maritime security regulations and industry best practices may be limited. This places the SSSAC at a disadvantage in their ability to effectively interpret existing standards against the inquiries into risk and performance based adjustments requested by Florida ports' security management. SSSAC membership should be reconfigured to include:

-
- Greater representation of maritime security and operations professionals;
 - More frequent standards review meetings; and
 - A timeline for SSSAC adjudication, recommendation, and response to seaport requests for interpretation and application of seaport security standards.

| Identification of Applicable State & Federal Regulations | |
|---|---|
| <p>Introduction</p> | <p>State Statute Overview: Florida Statute (FS) 311.12 - Seaport Security, was originally promulgated in 2000 in response to a statewide security assessment of Florida's seaports conducted by Camber Corporation on behalf of the Executive Office of the Governor's Office of Drug Control (ODC). This study focused on the primary threats to Florida's commerce at the time, which were:</p> <ol style="list-style-type: none"> 1. Drug Smuggling; 2. Cargo Theft; 3. Money Laundering, and 4. Internal Conspiracies. <p>The <i>Camber Report</i> outlined a number of recommendations that, when acted on by the Florida Legislature, provided a codified system of minimum security standards, practices, and procedures designed to create a uniform, effective, and secure operating environment for maritime commerce in Florida. Since 2000, FS 311.12 has been modified a number of times to provide guidance and clarity, and address deficiencies to the FS 311.12 standards and performance objectives.</p> |
| <p>Combined Physical Security Vulnerability & Operational Analysis</p> | <p>Federal Statute Overview: The U.S. Maritime Transportation Security Act (MTSA) of 2002 was promulgated by the federal government in response to the events of 9/11, and focuses on the protection of the commercial maritime facilities, vessels, and other facilities and operations from terrorist and criminal threats. The U.S. Coast Guard is responsible for oversight and enforcement of implementation of the federal maritime security standards and practices, which are outlined in 33 CFR part 105 (Facilities), and Navigational Vessel Inspection Circular (NVIC) 03-03, Change 2.</p> |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|---|--|
| <p>Security Standards</p> <p>Revised Definition of State Standards: FS 311.12 (2009) identifies, by reference, the minimum security standards against which Florida's commercial seaports are evaluated for compliance. The standards are not included in the legislation itself, but are identified and interpreted for application in the following documents:</p> <ol style="list-style-type: none"> 1. Port Security Standards Compliance Plan (2001); 2. Seaport Security Data Collection Uniform Guidelines for Field Inspection Activity (2009); and 3. Florida Department of Law Enforcement (FDLE) Special Agent in Charge (SAC) notes and in/out brief guidelines. | <ol style="list-style-type: none"> 1. Restricted Area Definitions: Aligning state and federal definitions of secure and restricted areas within a seaport. 2. Area Exemptions: Allowing all or part of a Florida commercial seaport to be exempted from the seaport security standards. 3. Transportation Worker Identification Credential (TWIC): Establishing the federal TWIC as the only credential authorized for use by the seaports when granting access to secure and restricted access areas. 4. State Background Check: Maintaining a requirement for a criminal history background check of crimes committed in Florida when determining access eligibility for secure and restricted access areas. 5. Disqualification Standards: Aligning state and federal criminal offenses that disqualify a person for unescorted access to secure and restricted access areas under the TWIC program. 6. Access Eligibility Reporting System (AERS): Establishing an AERS program that provides a centralized, secure database for use by seaports when granting or denying persons access to secure and restricted access areas; 7. TWIC Eligibility Affidavit: Creating an affidavit process for determining access eligibility for TWIC holders that reduces and consolidates state fees for port workers. <p>Analysis: Conflicts between the state statute, guidance related to interpretation of state minimum security standards, and federal standards do not readily support the seamless alignment of state and federal security seaport standards and practices. The minimum security standards continue to be based on the Florida Seaport Security Assessment 2000, as set forth in the Port Security Standards Compliance Plan (2001).</p> |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|---|--|
| <p>Security Standards</p> <p>Definition of Federal Standards: MTSA identifies the requirements for the implementation of preventive security measures to protect commercial U.S. seaports, U.S.-flagged vessels, and Outer Continental Shelf (OCS) platforms. Guidelines for the implementation and enforcement of security performance-based standards and practices are identified in 33 CFR part 105, and NVIC 03-03 change 2.</p> | <p>The Maritime Transportation Security Act (MTSA) of 2002 is the federal regulation that establishes minimum security standards for application to US commercial seaports. MTSA was promulgated subsequent to FS 311.12 and, as such, is in conflict with the state standard in that:• MTSA applies to all commercial US seaports that receive commercial maritime vessels, 100GWT and above, from international waters;• FS 311.12 applies only to the Florida's public, commercial seaports identified in FS 311.09;• The US Coast Guard is responsible for oversight and enforcement of the implementation standards and practices, which are based on an evaluation of the credible threats and risks associated with each port;• The Florida State Legislature established the Florida Department of Law Enforcement (FDLE) by as the state agency responsible for conducting FS 311.12 compliance audits against the prescriptive standards identified in the Port Security Standards Compliance Plan;• MTSA was developed to protect seaports and maritime commerce primarily against the threat of terrorist attack;• FS 311.12 was developed in response to a study that identified drug smuggling and cargo theft as the primary threats facing Florida's commercial seaports;• Commercial seaports that fail to achieve the MTSA compliance requirements may be subject to sanctions including, but not limited to: monetary penalties of up to \$25K, and withdrawal of USCG authorization to conduct business in the commercial maritime environment. • Florida seaports that fail to achieve "substantial compliance" with state seaport security standards are subject to having their findings of non-compliance reported to the state legislature.</p> |
| <p>Identification of Applicable Seaports</p> <p>FS 311.12 Applicable Seaports: State regulation applies only to the 14 commercial seaports specifically identified in the referenced state statute. <i>FS 311.09 (1)</i></p> | <p>The state's seaport security statute is not applicable to commercial maritime facilities or activities outside of the 14 specifically identified by the state Legislature. Limiting the application of existing state maritime security standards and practices to the 14 identified commercial ports is inconsistent with the intent of legislation, conflicts with federal requirements applied to maritime facilities in the same geographic jurisdiction, creates conflicts with road and rail carriers who support activities at ports subject to state and / or federal standards, and does not readily support the alignment of state and federal practices.</p> |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|---|---|
| <p>Security Standards</p> <p>MTSA Applicable Seaports: The federal statute and its supporting guideline documents are applicable to seaports, vessels, and activities not addressed by state statute. 33 CFR 105.105</p> | <p>A broad range of maritime facilities, vessels, and activities fall within the U.S. Coast Guard's purview for compliance with the federal statute:</p> <ol style="list-style-type: none"> 1. Facilities subject to 33 CFR part 126: Handling of Dangerous Cargo at Waterfront Facilities, part 127: Waterfront Facilities handling Liquefied Natural Gas and Liquefied Hazardous Gas, or part 154: Facilities Transferring oil or Hazardous Material in Bulk; 2. Facilities that receives vessels certificated to carry more than 150 passengers except those vessels not carrying and not embarking or disembarking passengers at the facility; 3. Facilities that receives vessels subject to the International Convention for Safety of Life at Sea (SOLAS), 1974, chapter XI; 4. Facilities that receive foreign cargo vessels greater than 100 gross register tons; 5. Facilities that receive U.S. cargo vessels, greater than 100 gross register tons, subject to 46 CFR chapter 1, subchapter 1, except for those facilities that receive <i>only</i> commercial fishing vessels inspected under 46 CFR part 105; 6. . Barge fleet facilities that receive barges carrying that receive barges carrying, in bulk, cargoes regulated by 46 CFR chapter 1, sub chapters D or O, or Certain Dangerous Cargoes (CDC). |
| <p>Port/Facility Security Plans</p> <p>State Standard: FS 311.12 (1) (a), (3) (2009) requires that each seaport listed in FS 311.09 adopt and maintain a security plan specific to that seaport, which:</p> <ol style="list-style-type: none"> 1. Provides for a secure seaport infrastructure; 2. Promotes the safety and security of state residents and visitors to the port; and 3. Promotes and supports the flow of legitimate trade and travel. | <p>The security objective related to FSPs, identified in the 2009 Security Data Collection Uniform Guidelines for Field Inspection Activity, focuses on the plan review, approval, and revision process, and does not provide a template for the structure and content of the report. The lack of standardization of maritime FSP nomenclature, format, contact, and review and approval process does not currently support alignment between state and federal regulations, and often results in the preparation and maintenance of redundant and conflicting security plan documentation.</p> |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|--|---|
| Security Standards | |
| <p>Federal Standard: NVIC 03-03, Change 2 outlines the MTSA Facility Security Plan (FSP) Implementation Process Methodology that addresses:</p> <ol style="list-style-type: none"> 1. FSP Review Process; 2. FSP Submission and Review; 3. U.S. Coast Guard Captain of the Port (COTP) Review and Approval Process; and 4. Implementation of FSP Inspection Cycles. | <p>NVIC 03-03 Change 2 provides specific guidance on:</p> <ol style="list-style-type: none"> 1. The information required for inclusion in Facility Security Plans (FSP) for MTSA regulated facilities; 2. The recommended FSP format and language content; 3. Detailed guidance on the specific items evaluated in compliance audit for each component of the FSP; 4. Sample audit report forms that illustrate the USCG's standardized format for documenting compliance audit results; 5. The process for submission of Alternate Security Program (ASP) and Equivalency or Waiver Requests for USCG review and adjudication; 6. A USCG Facility Security Spot Check Guide template. |
| Identification of Secure & Restricted Areas | |
| <p>State Standard: FS 311.12 (4)(a) (2009) includes revisions from previous iterations of this statute that specifically mandates aligning state definitions of secure and restricted access areas within a seaport with federal definitions.</p> | <p>The definitions outlined in the Port Security Standards Compliance Plan (2001) remain the standards against which compliance with state requirements is interpreted. The continued use of the compliance guidelines in the Port Security Standards Compliance Plan (2001) does not support the desired alignment of definitions and compliance measures.</p> |
| <p>Federal Standard: 33 CFR 105.405(a): Clearly identifies the criteria for the identification, designation, posting, and protection of secure and restricted access areas.</p> | <p>Federal standards regarding the identification of secure and restricted areas are risk and performance based. The federal statute requires the conspicuous posting of signs that:1. Describe the security measures in effect;2. States that entering the facility is deemed valid consent to screening or inspection;3. Failure to content or submit to screening or inspection will result in denial or revocation of authorization for entry.</p> |
| Identification of Exempted Areas | |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|---|---|
| Security Standards | |
| <p>FS 311.12 (2009) provides authority for FDLE to exempt all or part of a seaport listed in FS 311.09 from the security standards and requirements, if it determines that activity associated with the seaport, or part of the seaport, is not vulnerable to criminal or terrorist activities.</p> | <p>Interviews with Florida port security management personnel indicates that the state process for the identification and granting of area exemptions is time consuming, is vulnerable to the subjective analysis of FDLE in their interpretation of the applicability of the standards used to evaluate the threats and associated risk profile, and is not as responsive to the needs of the port as the federal process.</p> <p>Alignment of the state and federal processes for this requirement may be difficult, as the state-mandated process and authority for FDLE's evaluation of exempted areas is specifically outlined in the state statute, which may not be modified without legislative action to modify or eliminate this element of FS 311.12 (2009).</p> |
| ID/Access Control Badges | |
| <p>State Eligibility: Standards for determining eligibility for issuance of a port ID / access control badge is identified in minute detail in the Port Security Standards Compliance Plan (2001) - FSA 311.12 (2001)</p> | <p>FS 311.12 (2009) establishes TWIC as the only credential authorized, for access into Florida's seaports' restricted areas. However, the standards for the issuance and use of Florida port IDs, based on FDLE-conducted criminal background checks as outlined in the Port Security Standards Compliance Plan (2001), are still applicable. The FDLE-conducted criminal background checks are separate and distinct from the background checks conducted for issuance of the federal TWIC, and require payment of a fee for initial issuance, renewal, or replacement of ID / Access Control Badges. The standards for eligibility of ID / Access Control Badges applicable to Florida's ports are confusing and conflicting, and impose a financial burden on port employees, vendors, and visitors who are required to comply with the state-mandated "5 in 90" requirement for acquisition of a Florida port ID / Access Control Badge.</p> |
| <p>Federal Eligibility: MTSA establishes TWIC as the accepted ID.</p> | <p>The conflicting background investigation and eligibility requirements, combined with the current lack of sharing of information on disqualifying activities between federal and state agencies responsible for conducting ID / Access Control Badge screening activities, creates significant confusion and dissatisfaction among the populations requiring access to Florida's ports. The current mechanism for conducting criminal background checks against differing criteria for disqualification does not support the effective alignment of federal and state standards for this requirement.</p> |
| TWIC Possession & Retention | |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|--|---|
| Security Standards | |
| <p>State Requirement: FS 311.12 (2009) mandates that all persons seeking authorization for unescorted access to secure and restricted areas of a Florida seaport must possess a valid TWIC.</p> | <p>FS 311.12 (2009) specifically establishes TWIC as the only credential authorized for use by Florida's seaports, when granting access to secure and restricted access areas. This is intended to support the alignment of state and federal definitions of secure and restricted access, and the efficient, controlled access to ports for maritime commerce. However, FS 311.12 (4) (a) also must comply with the minimum security standards in subsection (1) which are defined in the Port Security Standards Compliance Plan (2001). These prescriptive standards, and associated requirements for FDLE-conducted criminal background check against state disqualification standards, conflict directly with the stated intent of the Legislature.</p> |
| <p>Federal Requirement: NVIC 03-07 outlines the requirements, standards, and procedures for the acquisition and retention of a TWIC.</p> | <p>NVIC 03-07 identifies the process for enrollment and issuance of TWIC. This includes the conduct of an FBI-conducted security threat assessment against federal criteria for disqualification, payment of a fee which covers the cost of enrollment, security threat assessment, and credential production and delivery. Federal criteria for disqualification of a TWIC are not the same as the state disqualification criteria required for FDLE-conducted criminal background investigations. In addition, personnel requiring access to Florida's ports are required to undergo a state background check, pay dual fees, and be issued both a state and federal credential for access into Florida's ports. This specifically conflicts with the intent to align state and federal requirements for access to Florida seaport secure and restricted areas.</p> |
| Access Eligibility Reporting System (AERS) | |
| <p>State Mandate: Established by the Legislature in FS 311.12 (2009) FS 311.12(5).</p> | <p>The AERS, when implemented, will be a centralized, secure system used to collect and maintain fingerprints and other biometric data, or other means of identifying persons authorized to enter a secure or restricted area of a Florida seaport. It also addresses receiving and transmitting information between Florida's seaports, area of authorized access and suspensions or revocations. It also requires a \$50 fee to cover administrative. Study participants consistently expressed significant dissatisfaction with charging a fee for a system that has not yet been fully developed or implemented.</p> |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|--|--|
| Security Standards | |
| Federal Mandate: Creation of this program is specific to the Florida statute. | Although the federal TWIC process includes the collection and maintenance of similar biometric identification data, each applicant's qualification or disqualification for receipt of a TWIC is based on federal disqualification standards. No mechanism exists for the transmission or sharing of data on disqualified applicants between federal and state investigative authorities. |
| Access Gates & Gate Houses | |
| State Standard: Prescriptive construction standards identified in the Port Security Standards Compliance Plan (2001) FS 311.12(4): Access Gates & Gatehouses. | FS 311.12 as outlined in the Port Security Standards Compliance Plan (2001) prescribes the standards for construction, equipment and manpower resources, and operations. |
| Federal Standard: Performance-based standard utilizing risk-based physical security measures for access control. | The federal standards for the construction, resources, and operation of seaport access gates and gate houses are subjective, and are based on ongoing assessment of risks to port operations associated with the identified credible threats. |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|---|---|
| Security Standards | |
| Designated Parking | |
| State Standard: Compliance requirements are identified in the Port Security Standards Compliance Plan (2001) FS 311.12(5): Designated Parking. | FS 311.12 requires a color-coded gate pass and / or decal system. The intent of the state standards is consistent with that of its federal counterpart. It is important to note that some seaports do not implement a car decal system, stating that it is more important to vet individuals at entry points, rather than their vehicle. |
| Federal Standard: Identified in 33 CFR, part 105.269 | Federal requirements for designated parking areas are included as a security measure for restricted areas, and compliance is based on functional achievement of the security objective rather than the detailed, prescriptive state requirements. |
| Fencing & Barriers | |
| State Standard: Prescriptive construction standards identified in the Port Security Standards Compliance Plan (2001) FS 311.12(6): Fencing. | The state minimum security standards specify the type of materials used and construction of fencing. The compliance audit focuses more on meeting the specific letter of the standards rather than the general performance objective of security fencing and barriers. |
| Federal Standard: 33 CFR 105.255: Security Measures for Access Control | Federal standards provide performance-based security objectives for measures appropriate to: <ol style="list-style-type: none"> 1. Designate restricted areas and provide appropriate access controls for those areas; 2. Identify access points that must be secured or attended to deter unauthorized access; 3. Deter unauthorized access to the facility and to designated restricted areas within the facility |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|---|---|
| Security Standards | |
| Lighting | |
| <p>State Standard: Prescriptive standards for lighting and illumination identified in the Port Security Standards Compliance Plan (2001) FS 311.12(7): Lighting.</p> | <p>The state minimum security standards includes prescriptive guidance on the type of lighting technologies to be used, and areas within the port required to have lighting, and the levels of illumination associated with lighting requirements for specific areas regardless of its impact on the environment or navigation.</p> |
| <p>Federal Standard: 33 CFR part 105.275: General requirements for the monitoring of secure and restricted areas, and operations at all maritime security (MARSEC) levels.</p> | <p>Federal standards requires that FSPs provide a description of security measures in place for the continuous monitoring of the port and its approaches, including lighting and illumination sufficient to support that activity. The federal standards also include the provision to limit lighting effects, such as glare, and their impact on safety, navigation, and other security activities at the port.</p> |
| Security Signage | |
| <p>State Standard: Prescriptive standards for signage are identified in the Port Security Standards Compliance Plan (2001): Use of Signs.</p> | <p>The state minimum security standards include specific guidance on the format and content required for compliance with this state standard. This is generally consistent with, and readily supports, alignment with the federal standards for signage.</p> |
| <p>Federal Standard: 33 CFR part 105.255: Security Measures for Access Control:</p> | <p>Requires the conspicuous posting of signs that describe security measures currently in effect at the port, and clearly state that:</p> <ol style="list-style-type: none"> 1. Entering the facility is deemed valid consent to screening or inspection; and, 2. Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to enter. |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|---|---|
| Security Standards | |
| Intrusion Detection & Monitoring Systems | |
| State Standard: FS 311.12 (22) (2001): Intrusion Detection System. | The Port Security Standards Compliance Plan (2001) includes guidance on the technological capabilities, placement, and use of CCTV systems for use in monitoring restricted areas and the approaches to those areas. |
| Federal Standard: 33 CFR Part 105.275: General requirements for the use of security systems and equipment for intrusion detection and monitoring of the port's approaches and restricted areas at each MARSEC level. | Requires a description of each port's use of layered security measures that have the capability to continuously execute the security monitoring function for commercial seaports. Applicable security systems include security guards, waterborne patrols, automatic intrusion-detection devices, surveillance equipment, or any other applicable security measures and technologies. |
| Security (Planning) Committees | |
| State Standard: FS 311.12 (11) (2001): Standing Security Committee. | The Port Security Standards Compliance Plan (2001) requires each seaport to sponsor / conduct a regularly scheduled forum at which all stakeholders in port security are invited to participate and discuss security issues. |
| Federal Standard: 33 CFR part 103: Area Maritime Security | <p>33 CFR Part 103 establishes the US Coast Guard Captain of the Port (COTP) as the Federal Maritime Security Coordinator (FMSC), and establishes the FMSC's authority to establish, convene, and direct the Area Maritime Security Committee (AMSC) to:</p> <ol style="list-style-type: none"> 1. Continually assess security risks to the port; 2. Determine appropriate risk mitigation strategies; 3. Develop, revise and implement the Area Maritime Security Plan (AMSP) 4. Communicate security threats and changes in the Maritime Security (MARSEC) levels to port stakeholders. <p>AMSC membership: USCG, Federal, State, and local law enforcement, emergency response organizations, port executive and security management, etc.</p> |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|--|---|
| Security Standards | |
| Security Standard Operating Procedures (SOPs) | |
| State Standard: FS 311.12 (13) (2001): Standard Operating Procedures | <p>The Port Security Standards Compliance Plan (2001) mandates that seaport management provide a current security manual for its facility that includes:</p> <ol style="list-style-type: none"> 1. Standards of conduct; 2. Responsibilities of appropriate security and management personnel; and 3. Definitive statement of management expectations of security force personnel; <p>The state-mandated security SOPs are generally consistent with federal requirements for specific security policies, procedures, and practices.</p> |
| Federal Standard: 33 CFR 105.405: Format and Content of the Facility Security Plan. | <p>Federal statute requires that the FSP include documented procedures for ensuring:</p> <ol style="list-style-type: none"> 1. A Facility Security Officer (FSO) is designated in writing; 2. Procedures for conducting Facility Security Assessments (FSA) are implemented; 3. SOPs for port personnel, with and without specific security duties, execution of their functions; and 4. Implementation of port security policies and procedures at each maritime security (MARSEC) level. |
| Law Enforcement Presence | |
| State Standard: FS 311.12 (14) (2001) Law Enforcement Presence, | <p>The Port Security Standards Compliance Plan (2001) requires each Florida port to ensure the routine, scheduled presence of sworn law enforcement personnel at Florida's seaports, and recommends the permanent assignment of a dedicated full-time unit of sworn law enforcement officers to each port. This requirement has been a catalyst for the increase in security spending for sworn law enforcement officers at Florida's ports.</p> |
| Federal Standard: N/A | <p>Since commercial seaports are border entry points, numerous federal officers are present at Florida's seaports, including, but not limited to: U.S. Customs and Border Protection (CBP); Immigration and Customs Enforcement (ICE); and the FBI. Despite the presence of federal officers, the state statute requires the presence of state-certified law enforcement officers for security patrols and criminal incident first response.</p> |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|---|---|
| Security Standards | |
| Security Guard Force | |
| <p>State Standard: FS 311.12 (15) (2001): Security Guards.</p> | <p>FS 311.12 (2009) created the Seaport Security Officer (SSO) qualification, Training, and Standards Coordinating Council to identify the qualifications, training, and standards for seaport security officer certification, and recommended a curriculum of at least 218 hours of initiation certification training to conform to security requirements under the MTSA. However, until the recommended curriculum is reviewed and approved by the Legislature for implementation, seaport security guard force personnel must comply with the training, certification, and employment requirements outlined in The Port Security Standards Compliance Plan (2001), and must be properly trained to be a state-certified Class D or Class G License holder.</p> |
| <p>Federal Standard: 33 CFR 105.210: Facility Personnel with Security Duties.</p> | <p>The federal statute requires specific training for facility personnel with specific security duties, including contracted security guard force personnel. The state requirement for guard force personnel to be certified Class D or Class G license holders is above and beyond federal standards, but does not hamper the alignment of state and federal standards for security guard force personnel.</p> |
| <p>Certified Seaport Security Officer Detention Authority</p> | |
| <p>State Standard: FS 311.124: Trespassing, Detention by a Certified Seaport Security Officer.</p> | <p>FS 311 (2009) authorizes any Class D or Class G seaport security officer certified under MTSA and FS 311.122 guidelines, who has probable cause to believe that a person is trespassing in a seaport's designated secure or restricted area, to detain such persons in a reasonable manner, for a reasonable period of time pending the arrival of a law enforcement officer.</p> |
| <p>Federal Standard: Not applicable</p> | <p>This requirement is specific to the state legislation, but in no way diminishes the relationship between the state-certified seaport security officers and federal law enforcement officers that may be stationed and operate at Florida's seaports.</p> |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|---|---|
| Security Standards | |
| Security Training, Drills & Exercises | |
| State Standard: FS 311.123: Maritime Domain Security Awareness Training Program. | <p>FS 311 (2009) mandates the creation of a maritime domain security awareness training program for delivery to all personnel employed within a seaport's geographic boundaries (inside the fence), regarding the security procedures required of them to implement the seaport security plan. The training curriculum must include security training requirements outlined in 33 CFR part 105, and be designed to enable Florida's seaports to meet the training, drill, and exercise requirements of the federal standards, in accordance with policies and procedures included in each port's seaport security plan.</p> |
| Federal Standard: 33 CFR 105.210: Facility Personnel with Security Duties; 33 CFR 105.215: Security Training for all Other Facility personnel; and 33 CFR 105.220: Drills and Exercises. | <p>The federal statute specifies requirements for training and certification of MTSA-mandated maritime security professionals, (e.g. Facility Security Officers, Company Security Officer, and Vessel Security Officer); port personnel with specific security duties; and, all other port personnel. The statute identifies specific subjects for instruction drawn from the U.N.'s International Ship and Port Facility Security (ISPS) Code. FS 311.12 (2009) requires alignment of state maritime security training and certification standards with those identified in the federal statute.</p> |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|---|--|
| Security Standards | |
| Maritime Domain Security Awareness Training Program | |
| <p>State Standard: FS 311.123: Maritime Domain Security Awareness Training Program.</p> | <p>This requirement is redundant with the requirement for Security Training, Drills & Exercises previously listed. FS 311 (2009) mandates the creation of a maritime domain security awareness training program for all personnel employed within a seaport's geographic boundaries, about the security procedures required of them for implementation of seaport security plan required under FS 311.12(3). This training curriculum must include security training requirements outlined in 33 CFR part 105, and be designed to enable Florida's seaports to meet the training, drill, and exercise requirements of the federal standards, in accordance with policies and procedures included in each port's Seaport Security Plan (SSP).</p> |
| <p>Federal Standard: 33 CFR 105.210: Facility Personnel with Security Duties; 33 CFR 105.215: Security Training for all Other Facility personnel; and 33 CFR 105.245: Declaration of Security.</p> | <p>Maritime Domain Awareness is an integral component of the federally-mandated security training and programs for incident response, management, and recovery operation at each MARSEC level.</p> |
| Information Security (INFOSEC) | |
| <p>State Standard: FS 311.13: Certain Information Exempt from Disclosure.</p> | <p>Per FS 311.12, SSPs are exempt from Article 1 of the State Constitutional requirement for public access to certain types of information. In addition, photographs, maps, blueprints, drawings, and similar materials that depict critical seaport operating facilities are exempt from Article 1 of the State Constitution, to the extent that a seaport reasonably determines that such items contain information that is not generally known, and that could jeopardize the security of the seaport. However, information relating to real estate leases, layout plans, blueprints, or other relevant information is not included in this exemption.</p> |
| <p>Federal Standard: 49 CFR 1520: Protection of Sensitive Security Information (SSI).</p> | <p>The standards and requirements for the protection of SSI is outlined in this federal regulation, which roughly corresponds to the definitions included in FS 311.13.</p> |
| Loose Cargo Storage | |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|---|--|
| Security Standards | |
| <p>State Standard: FS 311.12 (2001).</p> | <p>Section 18 of the Port Security Standards Compliance Plan (2001) addresses the specific requirements for cargo stored in open areas, palletized, or stacked cargo stored in warehouse facilities. Compliance focuses on the letter of the standards, and does consider credible threats, value of the materials protected, or additional measures in place to provide layered security for the facility and its operations.</p> |
| <p>Federal Standard: 33 CFR 105.265: Security Measures for Handling Cargo.</p> | <p>The federal statute requires documentation of procedures for the appropriate screening, handling, and storage of cargo at each security level. Requirements are based on the identified credible threats, risks, and operational requirements of each port and the nature of the respective cargo. Prescriptive state standards do not recognize layered security measures as providing an acceptable level of security relative to the nature of the cargo and current MARSEC level.</p> |
| <p>High-Value/Dangerous Cargo Handling & Storage</p> | |
| <p>State Standard: FS 311.12 (2001).</p> | <p>Section 19 of the Port Security Standards Compliance Plan (2001) defines High Value Cargo, and addresses the specific security requirements its storage. Compliance with this requirement does not include consideration of the credible threats; value of the materials protected, or layered security measures in place.</p> |
| <p>Federal Standards: 33 CFR 105.265: Security Measures for Handling Cargo part 126: Handling of Dangerous Cargo at Waterfront Facilities part 127: Waterfront Facilities handling Liquefied Natural Gas and Liquefied Hazardous Gas part 154: Facilities Transferring oil or Hazardous Material in Bulk</p> | <p>The federal statutes detail the procedures and documentation required for the appropriate screening, handling, and storage, and transfer of high-value or dangerous cargo at each security level. These requirements are based on the identified threats, risks, and operational requirements of each port and the nature of the respective cargo. The prescriptive state standards do not recognize layered security measures as providing an acceptable level of security relative to the nature of the cargo and current MARSEC level.</p> |
| <p>Equipment Control</p> | |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|---|---|
| Security Standards | |
| State Standard: FS 311.12 (2001). | Section 20 of the Port Security Standards Compliance Plan (2001) provides guidance on security measures for port cargo handling equipment. |
| Federal Standard: 33 CFR 105.305 Facility Security Assessment Report. | The federal standard requires facility security assessments to identify the vulnerabilities in the physical, structural, procedural, and personnel practices identified at each seaport. This includes an evaluation of the security measures in place to protect each port's critical infrastructure and key assets essential to ensure the safety and security of commercial operations. |
| Cruise Operations Security | |
| State Standard: Port Security Standards Compliance Plan (2001) (21) (2001). | This state standard references the requirement for Florida's seaports compliance with U.S. Coast Guard regulations identified in 33 CFR part 120 (Security of Passenger Vessels), and 33 CFR part 128 (Security of Passenger Terminals). FS 311.12 (2009) addresses alignment of state and federal definitions and standards for secure and restricted areas thus eliminating previous these conflicts. However, FDLE Inspectors reportedly continue to inspect the ports using outdated definitions of restricted areas that do not match federal definitions. |
| Federal Standard: 33 CFR, Part 105. | Federal standards identified in 33 CFR provide guidance on performance objectives and requirements for all facilities subject to MTSA. In addition, 33 CFR 128 (Security of Passenger Terminals) provides additional guidance on performance objectives and requirements to be implemented by passenger cruise terminal owner/operators. |
| Waiver from Security Requirements | |

| Security Objective | Analyses Overlaps/Conflicts/Alignment |
|---|---|
| Security Standards | |
| <p>State Standard: FS 311.12(8) (2009).</p> | <p>ODC and FDLE may modify or waive any physical facility requirement or other minimum security standard requirements as identified in the Port Security Standards Compliance Plan (2001), upon determination that the purposes of the standards have been reasonably met or exceeded by the seaport requesting the modification or waiver. However, the waiver determination is subject to a process that is not as responsive to port needs as the federal process.</p> |
| <p>Federal Standard: NVIC 03-03, Ch 2, Enclosure (9) Guidance for Submission of Alternative Security Programs, Equivalency and Waiver Requests.</p> | <p>Owner / operators of facilities subject to compliance with the requirements of 33 CFR part 105 are permitted to apply for a waiver of any requirements that the owner / operator considers unnecessary in light of the nature or operating conditions of the facility. The adequacy of each waiver request must include documentation supporting justification of the request for assessment by U.S. Coast Guards and assessed by appropriate U.S. Coast Guard personnel.</p> |
| <p>Seaport Security Standards Advisory Council (SSSAC)</p> | |
| <p>Florida's Legislature created the Seaport Security Standards Advisory Council (SSSAC) to review the minimum seaport security standards referenced in FS 311.12 (as outlined in the Port Security Standards Compliance Plan [2001]) for their applicability to and effectiveness in combating drug and terrorism threats to the state's commercial seaports. This element of FS 311.115 cannot be compared to any federal law, as the U.S. Coast Guard COTP has the authority to interpret port facility compliance with the performance-based standards provided in 33 CFR part 105, and NVIC 03-03, Change 2.</p> | <ol style="list-style-type: none"> 1. The legislatively-mandated requirement for an SSSAC convention to review and evaluate the standards at least every four years is not responsive to the needs of the port for interpretation of the existing standards on a more responsive basis; 2. The council consists of a minimum of 14 state government and industry representatives, of which only four have a regulatory requirement for specific knowledge and understanding of current maritime security regulations, threats, and operational requirements; 3. There is no timeline or deadline for the Legislature to act on the findings and recommendations of the council; 4. Current SSSAC composition, staffing, and process does not support the timely and effective review and adjudication of seaport application for interpretation of the validity of security standards as applied to specific port organization or operations. 5. Current SSSAC composition, staffing, and authorization does not support the evaluation of state minimum seaport security standards for alignment with their federal counterparts. |

6.4 Conclusion

The Florida Legislature's stated intent is to align the states seaport security standards and practices with their federal counterparts to eliminate conflicts in their interpretation and application, and reduce costs associated with unnecessary program redundancies. However, the ability to accomplish this alignment, with the present configuration of FS 311.12 (2009) and its supporting documents, is severely compromised. In addition, there is a lack of understanding throughout the Florida's commercial seaport community regarding the revised standards and performance requirements included in FS 311.12 (2009), the mechanism for their alignment with their federal counterparts, and FDLE's expectations regarding their implementation for effective compliance.

This comparative analysis of the state and federal seaport security standards, performance objectives and practices results in the following observations:

- The timely and seamless alignment of state and federal minimum seaport security standards, within the current legislative framework of the applicable Florida statutes and supporting guidance documentation, is unlikely to occur;
- Implementation of an alignment process would be greatly enhanced if the Florida Legislature revoked or voided the Port Security Standards Compliance Plan (2001) document, which is referenced in FS 311.12 (2009) for identification of the minimum seaport security standards applicable to Florida's commercial seaports;
- Limiting the application of seaport security standards to the seaports identified in FS 311.09 conflicts with federal requirements to establish and maintain a secure operating environment for all commercial seaports, their personnel, and operations;
- Modification of FS 311.115 to refine the composition of SSSAC and to expand its scope to include an active role in the alignment of state and federal seaport security standards, compliance requirements, and acceptable practices would enhance the possibility of successfully achieving that legislatively mandated objective; and
- Modification of FDLE's charter to include a component for outreach and education to Florida's seaports is necessary to support the desired alignment of state and federal seaport security standards and practices, and to ensure understanding of FDLE's expectations for compliance with the evolving requirements.

Lastly, it remains to be seen if maintaining state minimum security standards for a select, non-inclusive list of Florida commercial seaports provides any meaningful cost or operational deterrents to threats of terrorist or criminal activities above and beyond that provided through compliance with existing federal standards. In the event the legislative adjustment recommended to support the effective alignment of state and federal seaport security standards and practices is passed, the logical recommendation is for FS 311.12 and its supporting guidance documentation, be voided or revoked in favor of the uniform application of federal standards for all Florida commercial seaports.

Page Left Blank Intentionally

7.0 Combined Florida Physical and Operational Vulnerability Analysis

Contents of this Section have been classified as Security sensitive Information and have been removed from this publicly available copy. For more information of these sections please contact the Florida Office of Drug Control or Florida Department of Law Enforcement.

Page Left Blank Intentionally

8.0 Combined Florida Ports Risk Assessment Update

Contents of this Section have been classified as Security sensitive Information and have been removed from this publicly available copy. For more information of these sections please contact the Florida Office of Drug Control or Florida Department of Law Enforcement.

Page Left Blank Intentionally

9.0 Florida Ports Security Operations Costs Analysis

Contents of this Section have been classified as Security sensitive Information and have been removed from this publicly available copy. For more information of these sections please contact the Florida Office of Drug Control or Florida Department of Law Enforcement.

Page Left Blank Intentionally

10.0 TWIC FUPAC Analysis

10.1 Introduction

To effectively compare federal and state regulations regarding port ID and background checks, it is necessary to analyze the state requirements of Florida Uniform Port Access Credential (FUPAC) and Access Eligibility Reporting System (AERS) and the federal requirement of Transportation Workers Identification Credential (TWIC). Florida law requires public seaports through Florida Statute (FS) 311.12 to conform to state port security standards.

Through inspections, the Florida Department of Law Enforcement (FDLE) has the primary responsibility for determining the extent to which each seaport conforms to the standards. Federal law, through the Maritime Transportation Security Act of 2002 (MTSA), requires seaports to develop security plans which are reviewed and approved by the U.S. Coast Guard. Seaport officials and tenants have suggested that Florida's standards place an undue burden on the seaport community (stakeholders, port users, workers, etc.).

This section of the report examines the now defunct state requirement of FUPAC, its replacement, AERS, and the federal standards for TWIC as they relate to Florida's seaports. It also summarizes the views of stakeholders based on site visits, surveys, and telephone interviews. Recommendations are also provided.

10.2 Legislative Timeline

| | |
|-----------------------|---|
| November 1999 | Legislative Task Force: The Florida legislative task force on Illicit Money Laundering issued a report titled <i>Money Laundering in Florida: Report of the Legislative Task Force</i> . The report noted that while access was controlled at some ports, the efforts were not consistently applied. |
| September 2000 | Camber Report: The <i>Florida Seaport Security Assessment</i> , also known as the <i>Camber Report</i> indicated that port management should have a greater role in port tenant security operations. |
| 2000 | FUPAC: The Florida Legislature created section 311.12 Florida Statutes. FS 311.12 required the Florida Office of Drug Control in consultation with the Florida Seaport Transportation and Economic Development Council, the Florida Department of Law Enforcement, and local law enforcement agencies to develop a statewide security plan based on the Camber Report. The statewide security plan was required to establish statewide minimum standards for seaport security. Florida's public ports were required to develop individual seaport security plans and adhere to the standards. The requirement for FUPAC was created. The FUPAC required ports to conduct a state background check on port workers. |

| | |
|--------------------------|---|
| December 2000 | Fifteenth Statewide Grand Jury: The Fifteenth Statewide Grand Jury issued a report entitled <i>An Analysis of Florida's Drug Control Efforts</i> . The report stated that "...the majority of Florida's seaports are operated in a manner that encourages unlawful behavior, rather than discouraging it." The report recommended criminal background checks on seaport employees. |
| December 11, 2000 | Port Security Standards Compliance Plan: The Office of Drug Control delivered the <i>Port Security Standards Compliance Plan</i> that contained <i>prescriptive</i> standards relating to issues such as visitor access, access gates, parking, fencing, lighting and signage. |
| July 1, 2003 | MTSA: MTSA was passed that outlined <i>risk-based performance</i> -based standards for port facilities. The MTSA required credentialed merchant mariners and workers with unescorted access to secure areas of vessels and facilities to undergo a security threat assessment and receive a biometric credential known as the TWIC. |
| 2006 | TWIC: Roll out of the TWIC begins. Implementation of the FUPAC is placed on hold pending efforts to align the FUPAC and the TWIC. |
| June 4, 2009 | H.R. 2200 Transportation Security Administration (TSA) Authorization Act of 2010: The authorization act passes the U.S. House and now goes on to the U.S. Senate for debate. The act contains an amendment prohibiting separate security background checks for transportation security cards, unless necessitated by a compelling homeland security reason. |
| June 8, 2009 | H.R. 2200 TSA Authorization Act of 2010: The TSA Authorization Act is received in the Senate and referred to the Committee on Commerce, Science, and Transportation. |
| July 1, 2009 | AERS: Florida House Bill (HB) 7141 revised and updated security provisions for the state's seaports and, among other actions, eliminated FUPAC, and, in its stead, created AERS. A database for the ports to store state background information on port workers. The system is not yet operational. Note: If the TSA Authorization Act of 2010 passes US Senate vote, the background check required under the AERS will not be implementable. |

10.3 Recent Changes to FS 311.12

Previous iterations of Florida law (FS 311.12 [125]) required seaport workers to submit to a criminal background screening prior to obtaining a FUPAC. However, due to the federal legislation requiring TWIC, FUPAC was never implemented. Subsequent changes to Florida's legislation through House Bill (HB) 7141 eliminated FUPAC, and, in its stead, created AERS. HB 7141 also does the following:

- Establishes TWIC as the only credential authorized for use by the seaports listed in FS 311.09;
- Maintains a requirement for a criminal history background check of crimes committed in Florida when determining access eligibility for secure and restricted access areas; and
- Aligns state criminal offenses that disqualify a person for unescorted access to secure and restricted access areas with federal disqualifying offenses under the TWIC program, and creates an affidavit process for determining access eligibility for

TWIC holders that reduces and consolidates state fees for port workers.

While no ID badges are issued under the AERS, Florida's ports must conduct a Florida state criminal background screening prior to granting a port user regular access to a port. Such background screenings are occurring, and certain ports initially collected the AERS fee. However, at the time of writing, no ports were collecting the AERS fee. However, the issuance of a port ID continues to be contingent upon the successful completion of the state background screening, thus creating a de-facto FUPAC.⁴⁶

10.4 Relevant Legislative Components

AERS Enrollment Fee: A \$50 fee is required under AERS to cover the initial cost of entering the person into the system and an additional \$50 fee every five years thereafter to coincide with the issuance of TWIC. The fee covers all costs for entering or maintaining the person in the system including the retention and use of the person's fingerprint, other biometric data, or other identifying information. Seaports entering individuals into the system may charge an administrative fee to cover, but not exceed, the seaport's actual administrative costs for processing the results of the state criminal history check and entering the person into the system.⁴⁷

Eligibility: FS 311.12 was originally intended to provide a deterrent to drug trafficking and cargo theft, therefore, AERS has additional disqualifying offenses compared to TWIC.⁴⁸ Individuals seeking regular access to Florida's ports under AERS are disqualified from employment or unescorted access if convicted of the offenses within the previous seven years, or within five years of any incarceration, or supervision imposed as a result of the offense.

Waiver and Appeal Process: FDLE recently revised its guidelines for seaport workers who have been denied access to Florida's ports under AERS as provided in s.311.12 (7)(e).⁴⁹ Under these guidelines, FDLE submits the worker's waiver application to the Florida Parole Commission, which reverts with its findings to FDLE.

Criminal / Terrorism Background Check-Federal: The federal criminal and terrorism background check for all TWIC applicants involves a name and fingerprint analysis through the federal National Crime Information Center (NCIC) database.⁵⁰ The Federal Bureau of Investigation (FBI)

⁴⁶ Currently, individuals who visit one of Florida's publicly funded ports more than five days out of ninety (5 & 90 Rule), including workers applying for work at one of the ports, must apply for a Port ID badge. Port workers who require unescorted access to restricted areas at MTSA-regulated facilities are also required carry a TWIC. Most ports require workers to present their port ID badge at the port's access point.

⁴⁷ The AERS is under development, and not currently available for ports to access. This has led to the situation in which ports are required by statute to charge port users for a service that does not yet exist. A TWIC currently costs \$132.50 to which is added the AERS fee of \$50. The resulting cost to port users is \$182.50 every five years. However, ports may charge an administration fee, which is not established by statute. Therefore, the final cost to port users for the combined TWIC / AERS is unclear, and may vary from port to port.

⁴⁸ See Appendices for a list of disqualifying offenses under AERS.

⁴⁹ <http://www.fdle.state.fl.us/Content/getdoc/de17647d-7abf-4e82-87cc-721a52406517/Waiver-Guidelines.aspx>. Accessed January 17, 2010.

⁵⁰ Seaport Security: The Florida House of Representatives Committee on Homeland Security, Committee Meeting Packet (March 6, 2009).

conducts the checks, and also matches applicants' names against the U.S. terrorist watch list, as well as international terrorism sources such as Interpol.⁵¹ Data contained in NCIC is provided by the FBI, federal, state⁵², local and foreign criminal justice agencies, and authorized courts.⁵³

Criminal / Terrorism Background Check-State: The Florida fingerprint check is conducted through the Florida Crime Information Center (FCIC) database which captures state offense information (i.e., outstanding warrants) that is not always available in the federal system. Such information is available if a driver's license check is conducted upon entry into the facility. Further, FDLE's intelligence databases include violent crimes, gangs, narcotics and economic crime investigations, and domestic crimes.⁵⁴ Such local information may not be available in federal and international databases.

Federal Law: Federal law through MTSA requires seaport workers who need unescorted access to restricted areas to obtain a TWIC⁵⁵. As previously mentioned, although the FUPAC no longer exists, the requirement for state background checks and the associated costs do exist under the AERS.⁵⁶

TWIC Waiver and Appeal Process: The TSA established a waiver and appeal process for ineligible TWIC applicants.⁵⁷ Applicants may apply for waivers if disqualified due to offenses related to terrorism, treason, sedition, or espionage.⁵⁸ TSA grants waivers upon determining if an applicant poses no security threat.⁵⁹ Additional procedures are in place for immigration, U.S. residency, or mental competency-based denials.⁶⁰

As of January 13, 2010, 1,459,796 individuals have enrolled in TWIC. 1,339,069 TWICs have been activated. 67,490 applicants have been initially disqualified. 36,825 of those initially denied a TWIC have filed an appeal, and 35,882 appeals have been granted. 7,700 waivers have been requested, while 3,624 waivers have been granted.⁶¹

TWIC Card Readers: Currently, seaports do not have card readers at each port entrance capable of reading a TWIC. The TWIC can only be used for visual identity verification, and for 'spot checks' with hand-held

⁵¹ 49 CFR 1572.2(c)

⁵² Interviews with FDLE indicated that the TSA may not have full access to Florida's criminal databases, and that "hundreds, if not thousands of Florida's criminal records are not available to the TSA." For this reason FDLE does not support rescinding the requirement for a Florida State background check required by the AERS.

⁵³ <http://www.fas.org/irp/agency/doj/fbi/ncic.htm>. Accessed January 26, 2010.

⁵⁴ <http://www.fdle.state.fl.us/Content/getdoc/ed464270-a6c5-4737-8680-bae4518d8fea/StatementOfAgencyOrganization.aspx> Florida Department of Law Enforcement (FDLE) Statement of Agency Organization accessed January 26, 2010.

⁵⁵ P.L. 107-295.

⁵⁶ Through the course of this study, participants consistently reported that seaport users (employees, tenants, customers, potential clients, and other visitors) objected to the costs associated with obtaining two background checks.

⁵⁷ P.L. 107-295. See also 49 CFR Part 1515.7.

⁵⁸ 49 CFR 1572.103(a).

⁵⁹ *Id.* In determining whether to grant a waiver, TSA may consider the circumstances of the disqualifying offense, mitigation, restitution to victims, etc.

⁶⁰ 49 CFR 1515.5.

⁶¹ http://www.tsa.gov/assets/pdf/twic_dashboard.pdf. Accessed January 17, 2010.

TWIC scanners. The Department of Homeland Security (DHS) is conducting a pilot program to test the business processes, technology, and operational impacts required to deploy TWIC readers at secure areas of the marine transportation system. After the pilot program has concluded, DHS will issue final regulations that require deployment of TWIC readers that are consistent with the findings of the pilot program.⁶²

MTSA require the adoption of a nationwide transportation security card. In response, federal efforts led to the development of the TWIC. The goal of the TWIC program is to provide a single nationwide transportation industry access credential that, after completion of a screening process including background check, will signify eligibility for unescorted access to a facility.

The MTSA states that an individual can be denied a TWIC if they have been convicted within the preceding seven-year period or released in the last five years of a felony or found not guilty by reason of insanity of a felony that DHS believes could cause the individual to be a terrorism security risk to the U.S., or for causing a severe transportation security incident. The law does not specify those crimes. The law also notes that a TWIC may be denied for immigration violations or other terrorism risks.

The TWIC rule includes the following permanently disqualifying criminal offenses, crimes, and conspiracies:

espionage; sedition; treason; a terrorism crime, a transportation security incident crime, improper transportation of hazardous material; unlawful possession, use, sale, ...or dealing in an explosive or explosive device; murder; or violations of RICO (organized crime).

Individuals who have been involuntarily committed to a mental institution are considered a security threat and are disqualified.

Fourteen other crimes disqualify individuals if they were convicted within the previous seven years or incarcerated within five years. They are:

- assault with intent to murder;
- kidnapping or hostage taking;
- rape or aggravated sexual abuse;
- unlawful possession, use, sale....of a firearm or other weapon;
- extortion;
- dishonesty, fraud, or misrepresentation, including identity fraud;
- bribery;
- smuggling;
- immigration violations;
- lesser RICO violations;
- robbery;

⁶²https://www.fbo.gov/index?s=opportunity&mode=form&id=fec5f854ca020d58c63558acd8f35c3&tab=core&_cview=0 Accessed January 17, 2010.

-
- distribution, possession with intent to distribute, or importation of a controlled substance, including drugs;
 - arson; and
 - conspiracy.

The TWIC is valid for five years.

The TWIC rule is performance-based. Ports are given the ability determine which TWIC holders will be granted access to secure areas of their facility, however, ports are also required to implement TWIC into their existing access control systems and operations, purchase and utilize card readers, and update their approved security plans. Access control procedures and systems at facilities and vessels must recognize the credential and the information encrypted on it, so that the overall maritime network will be interoperable

Port ID Badge: According to the TWIC rule, if owner/operators choose to use a separate badge system, it must be coordinated with the TWIC requirements, such that notification to the owner/operators of changes in the individual's TWIC status are also reflected in the separate badging system.

10.5 Analysis

During the interviews, site visits, and teleconferences conducted for this study, participants were fairly consistent in expressing confusion regarding the effective implementation of the TWIC, port ID badges, and the new AERS⁶³.

New Federal Legislation: An amendment to the 2010 TSA Authorization Act prohibits states from requiring a separate security background check unless a compelling homeland security reason dictates a separate background check is necessary. The bill, while having already passed a U.S. House vote, is currently under consideration by the U.S. Senate.⁶⁴

Port Management: Florida seaport administrators were fairly consistent in reporting that final facility access should be granted to TWIC card holders after verification of a valid business purpose on the port. Most Florida seaports would issue a local port access card that grants various permissions to move about the port. In most cases, local port access cards are not recognized by other state ports.

Port management also indicated that while Florida has adopted the TWIC as the universal access control credential for all Florida ports subject to FS 311, FS 311 still requires that individuals entering ports on a regular basis receive a state background check. The TWIC was created by the federal government as an identification credential, not an access control credential as envisioned by the state of Florida.⁶⁵

FDLE: Representatives from FDLE consistently stated that two background checks are necessary given that the federal background check does not have access to Florida databases. Federal background check findings are not shared with FDLE, leaving FDLE blind as to which TWIC holders may have received their TWIC on a federal waiver. This has created a situation in which neither the federal nor the state entities charged with conducting background checks has access to each other's criminal history information. Such failure to communicate was one of the complicating factors that was identified by the *9/11 Commission Report* which found:

⁶³ One port involved in the study reported it was a signee to a Memorandum of Understanding in which three geographically proximate ports recognized the other ports' ID badge and related background check. With the passage of the AERS on July 1, 2009, the port reported it is withdrawing participation in the MOU, since it now issues 5-year badges as required by statute. At the time of writing, the other two ports in the MOU were not issuing 5 year badges.

⁶⁴ <http://castor.house.gov/News/DocumentSingle.aspx?DocumentID=151161>. Accessed January 18, 2009.

⁶⁵ Regarding port ID denials, one port, when queried if individuals denied port IDs were TWIC holders, the response was, "Probably not. We do not care if they have TWICs or not. We do not admit them." This indicates that, at least at some ports, the TWIC card is irrelevant. Upon analysis of the reasons for denial, a port's power to deny a port ID extends beyond AERS disqualifying offenses. For example, one individual was denied a port ID badge, not due to a disqualifying offense listed in AERS, but rather because the applicant "threw his wife out on the port." It is unclear from the port's response if criminal charges were filed in this matter. Such behavior, while certainly serious, may not have been grounds for denial / revocation under either TWIC or AERS. It is evident that ports have wide latitude to deny port IDs above and beyond the disqualifying offenses listed in the AERS or TWIC.

The combination of an overwhelming number of priorities, flat budgets, an outmoded structure, and bureaucratic rivalries resulted in an insufficient response to this new challenge.⁶⁶

Further, the 9/11 Commission Report recommended that guidelines be determined for “gathering and sharing information” in the new security systems that are needed, guidelines that integrate safeguards for privacy and other essential liberties. The apparent disconnect between federal and state background checks illustrates that the 9/11 findings and recommendations still resonate today.

Significantly, Florida is believed to be the only state that performs its own background checks on persons seeking access to restricted areas within its seaports. The federal government believes that the background checks performed by the TSA, and using the FBI’s criminal database prior to the issuance of a TWIC, are sufficient to protect seaports against the introduction of individuals that could pose a threat.

AERS Fee: In order to comply with the legislation, the Port of Miami began collecting the \$50 fee from Port ID applicants. It has since stopped the practice, and has returned the fees collected to the applicants. The requirement for collection of funds associated with implementation of the AERS system was erroneously scheduled to begin before the FDLE data collection mechanisms were in place thus creating confusion and additional work throughout the port community.

Flawed Alignment between AERS & TWIC: To avoid multiple background checks on the same individual, the Florida legislature directed FDLE to track TWIC holders who have received fingerprint-based FCIC background checks. However, under federal law, many port users are not required to have a TWIC to work on all facilities. This illustrates a lack of alignment between federal and state standards concerning “restricted” and “secure” areas.⁶⁷ Port management was consistent in reporting that the disqualifying crimes under both TWIC and AERS should be consistent with each other, and that a single background check should be sufficient to protect Florida’s ports.⁶⁸

However, additional disqualifying factors still exist under AERS, which indicates that AERS and TWIC, while more streamlined, are not yet completely aligned, thus creating confusion in the port community.

For TWIC holders, FDLE requires a background check against Florida’s criminal history databases. Non-TWIC holders who require regular

⁶⁶ The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. http://www.9-11commission.gov/report/911Report_Exec.pdf Accessed January 31, 2010.

⁶⁷ The City of Tampa operates a waste water treatment plant surrounded by public port property. (HB) 7141 requires that these workers obtain a TWIC, even though they are not bound by any Federal security regulations that would require a TWIC. The port authority estimates the up-front cost to the City of Tampa in excess of \$100,000.

⁶⁸ The US Coast Guard’s Captain of the Port for Sector Miami issued a waiver from the TWIC requirement for Port of Miami cruise terminal workers. This conflicts with FS 311, which requires all workers at Florida’s cruise terminals, which by statute are considered “restricted areas” to hold a TWIC and to be entered into the AERS.

access to restricted or secure areas of the port, whether escorted or not, are required by FDLE to submit to both national and state background checks.

At the time of writing, AERS has not been implemented. This is due, in large part, to the passage of federal legislation prior to the completion of a full implementation plan including related technology and training.

Information Sharing: The TSA does not provide information to states on the disqualification criteria against which a TWIC applicant may have been denied issuance of that credential, or if the TWIC was received through the waiver process.

Administrative Costs: Florida's ports must maintain a background check credentialing office and charge administrative fees to businesses and individuals to help defray administrative costs. Annual administrative costs at large seaports (i.e., Port Everglades, Jacksonville, Miami, Tampa) range from \$700,000 to \$1 million.

Florida Department of Law Enforcement: FDLE maintains that all previous existing standards remain in effect under HB 7141 (July 1, 2009), including a badge standard that the TWIC does not comply with. No federally-approved system is yet available to read TWIC cards, therefore the establishment and operation of the AERS component to track approved TWIC holders is further complicated.⁶⁹

Tenants: Tenants expressed their frustration regarding the costs and lost time associated with the dual background checks required to access Florida's ports. The implementation of AERS adds additional bureaucracy and costs that Florida's port users must bear.

In creating AERS, Florida becomes the only state that does not rely on the TWIC background check as sufficient to protect its seaports from individuals with questionable backgrounds from gaining access to restricted areas.

10.6 Recommendations

Pending Legislation: Pending legislation may prohibit Florida from conducting the AERS-required background checks, unless a compelling homeland security reason to do so is provided. It is in Florida's best interest to wait until the outcome of pending legislation prohibiting state background checks is known prior to implementing AERS.

Alignment: Should the AERS not be prohibited by pending federal legislation, an effective process should be developed to ensure that AERS is *truly* aligned TWIC evaluation criteria. The disqualifying factors

⁶⁹ Specifically, the TWIC does not comply with compliance standard 1 b. Picture IDs should be color coded or clearly identified by other means (e.g. hologram or symbol) to indicate areas to which access is authorized (e.g. docks, cargo yards, marine terminals, administration buildings, or unrestricted access).

for both AERS and TWIC should mirror each other to meet the intent of 311.12, and to ensure equivalency between federal and state background checks.

Information Sharing: One of the stated goals of the federal government is to facilitate information sharing. In a move toward accomplishing this goal, the Florida Legislature should determine how Florida felonies can be uploaded to the NCIC database.

11.0 Annexes

Annex A: Florida Statute 311.12

Page Left Blank Intentionally

Annex B: Maritime Transportation Security Act, 33 CFR, Part 105

Page Left Blank Intentionally

Annex C: 33 CFR, Part 128

Page Left Blank Intentionally

Annex D: NVIC 03-03, Change 2

Page Left Blank Intentionally

**Annex E: NVIC 03-07, related to the Transportation Worker Identification Credential
(TWIC)**

Page Left Blank Intentionally

Annex F: Seaport Security Standards Advisory Council (SSSAC) Recommendations

Page Left Blank Intentionally

Annex G: Florida Statute 311.12 Compliance Plan

Page Left Blank Intentionally

**Annex H: Seaport Security Data Collection Uniform Guidelines for Field Inspection
Activity, Effective July 1, 2009**