The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Military Affairs and Domestic Security Committee

BILL: PCS/SB 1470 (733872)

INTRODUCER: Military Affairs and Domestic Security Committee and Senator Dean

SUBJECT: Seaport Security

DATE: April 4, 2008 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Pardue	McElroy	MS	**Pre-meeting**
2.			CJ	
3.			TA	
4.			RC	
5.				
6.				

I. Summary:

This bill authorizes the Department of Highway Safety and Motor Vehicles to designate the U. S. Transportation Security Administration's Transportation Worker Identification Credential (TWIC) card as the Uniform Port Access Credential Card. The bill authorizes the department to set and collect a fee for entering a TWIC cardholder into the Uniform Port Access Credential System.

This bill creates section 311.125 (15) of the Florida Statutes.

II. Present Situation:

Federal Law

The federal government has authority over any public or private port facility located in, on, under, or adjacent to any waters subject to the jurisdiction of the U. S. The Maritime Transportation Security Act of 2002 (MTSA)[1] signed into law on November 25, 2002 established a port security framework in the aftermath of the terrorist attacks of September 11, 2001.

The MTSA requires the Coast Guard to conduct vulnerability assessments of vessels and facilities on or adjacent to U.S. waters. It mandates that a National Maritime Transportation Security Plan and regional Area Maritime Transportation Security Plans be developed and implemented by the Coast Guard for deterring and responding to transportation security

[1] Public Law 107-295.

incidents. Vessels and port facilities are required to have comprehensive security plans and incident response plans based on detailed Coast Guard vulnerability assessments and security regulations. Such security plans must be approved by the Coast Guard.

The law requires that access to security sensitive areas be limited through background checks and the issuance of transportation security cards. Persons accessing secure areas on vessels or facilities are required to undergo a background check.

A biometric transportation security card must be issued to individuals allowed unescorted access to a secure area of a vessel or facility. Under a recently released final federal rule, individuals are denied unescorted port access if convicted or found guilty by reason of insanity of certain felonies.[2] Permanently disqualifying felonies include:

- Espionage or conspiracy to commit espionage;
- Sedition or conspiracy to commit sedition;
- Treason or conspiracy to commit treason;
- A federal crime of terrorism;
- A crime involving a transportation security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption;
- Improper transportation of a hazardous material;
- Unlawful possession, use, or sale of an explosive or explosive device;
- Murder;
- Making a threat or maliciously conveying false information concerning an explosive or other lethal device;
- Violations of the Racketeer Influenced and Corrupt Organizations Act; and
- Conspiracy or attempts to commit any of the crimes listed above.

Certain felonies disqualify a person for unescorted port access for a period of seven years after conviction or found guilty by reason of insanity or for a period of five years after release if incarcerated for any of the following:

- Unlawful possession, use, sale, manufacture, import, export, or dealing in a firearm or other weapon;
- Extortion;
- Fraud excluding welfare fraud and passing bad checks;
- Bribery
- Smuggling;
- Distribution of, possessing with intent to distribute, or importation of a controlled substance;
- Arson;
- Kidnapping or hostage taking;
- Rape or aggravated sexual abuse;
- Assault with intent to kill;
- Robbery; and

[2] 49 CFR Part 1572

- Conspiracy or attempts to commit any of the crimes listed above.

Transportation Worker Identification Credential

The TWIC was established by Congress through the MTSA and is administered by the U. S. Transportation Security Administration (TSA) and the Coast Guard. TWICs are tamper-resistant biometric credentials that will be issued to all credentialed merchant mariners and workers who require unescorted access to secure areas of ports, vessels, or outer continental shelf facilities. It is anticipated that more than 750,000 workers including longshoremen, truckers, port employees and others will be required to obtain a TWIC.

Enrollment and issuance began at the Port of Wilmington, Delaware October 16, 2007 and will continue through calendar year 2008. To obtain a TWIC, an individual must provide biographic and biometric information such as fingerprints, sit for a digital photograph and successfully pass a security threat assessment conducted by TSA. Pre-enrollment is recommended as it is designed to save the applicant time by enabling them to provide their biographical information and make an appointment for in-person enrollment.

Currently, there are no regulatory requirements pertaining to the use of TWIC readers. However, initial testing and evaluation of TWIC readers will begin in calendar year 2008 as part of the pilot phase.[3]

Florida Law

In its final report issued in November of 1999, the Florida Legislative Task Force on Illicit Money Laundering recommended the establishment of minimum security standards for the state's seaports. The 2000 Legislature directed the Governor's Office of Drug Control Policy to develop a statewide security plan based on the Florida Seaport Security Assessment. The Office of Drug Control was directed to develop statewide minimum seaport security standards and each of Florida's seaports was required to develop individual security plans based on the statewide standards.[4]

The statewide minimum standards were enacted in 2001 in Chapter 112, Laws of Florida, and required the approval of individual seaport security plans by the Office of Drug Control and the Department of Law Enforcement.

Statewide Minimum Standards: Section 311.12, F.S., provides statewide minimum security standards for the following deepwater seaports: 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.[5]

[3] Source: Transportation Security Administration, http://www.tsa.gov/what_we_do/layers/twic/index.shtm
[4] Chapter 2000-360, Laws of Florida.
[5] Note: The public port portions of Fort Pierce and Port St. Joe are currently inactive to commercial operations and are exempted from compliance under s. 311.12 (1) (b). Should these ports resume commercial operations, they will be required to comply with the provisions of Chapter 311, F.S.

The statewide standards are set forth in the "Port Security Standards - Compliance Plan" (Compliance Plan) provided to the Legislature on December 11, 2000. Seaports subject to these standards must maintain a security plan that is tailored to meet the individual needs of their port and assures compliance with the statewide standards. As part of such security plan, a seaport shall designate unrestricted and restricted access areas within the seaport.[6] Persons working within or regularly entering restricted access areas are required to possess a Uniform Port Access Credential Card

Criminal History Checks: Section 311.12(3)(a), F.S., requires that a fingerprint-based criminal history check 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 is 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. Criminal history checks are performed at least once every 5 years on employees or others with regular access and the results of these checks are provided to the requesting seaport. The costs of the checks are consistent with the provisions of s. 943.053(3), F.S, and are paid by the seaport, employing entity, or by the person checked.

Each seaport security plan must identify criminal convictions or other criminal history factors that disqualify a person from either initial seaport employment or new authorization for regular access to seaport property or to a restricted area. Any person, who has within the past seven years been convicted, regardless of whether adjudication was withheld, for the following offenses, does not qualify for employment or access to restricted areas at a seaport:

- A forcible felony as defined in s. 776.08, FS.;
- An act of terrorism;
- Planting of a hoax bomb;
- Any violation involving the manufacture, possession, sale, delivery, display, use, or attempted or threatened use of a weapon of mass destruction or hoax weapon of mass destruction;
- Dealing in stolen property;
- Any violation involving the sale, manufacturing, delivery, or possession with intent to sell, manufacture, or deliver a controlled substance;
- Burglary;
- Robbery;
- Theft;
- Display, use, threaten, or attempt to use any weapon while committing or attempting to commit a felony;
- Any crime an element 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.[7]

A person who has been convicted for any of the offenses listed does not qualify for initial employment or authorized regular access to a seaport or restricted area unless after release from

[6] s. 311.12(2), F.S.
[7] s. 311.12(3)(c), F.S.

incarceration (and any post incarceration supervision), the person remains free from any subsequent conviction for such offenses for a period of at least seven years prior to the employment or access date under consideration.

Section.311.12 (3) (e), F.S., provides for a waiver procedure to allow unescorted access to an individual who is disqualified under s. 311.12(3) (c), F.S.

Florida Uniform Port Access Credential: Section 311.125, F.S., established the Uniform Port Access Credential System. This section requires each seaport identified in s. 311.09, F.S., to use the Uniform Port Access Credential and directed the Department of Highway Safety and Motor Vehicles to develop the system. The section further directed that the system conform, as closely as possible, with criteria established by the TSA for a TWIC and at a minimum consist of:

- A centralized, secure database for collecting and maintaining fingerprints and other biometric means of identity, and other means pertaining to personal identification of persons working on, or doing business at, a Florida seaport;
- A methodology for receiving and transmitting data to each port regarding access permissions;
- Technology required for each gate and portal at each seaport to be interactive with the Uniform Port Access Credential System during all hours of operation;
- The ability to identify persons who have violated the access requirements of s. 311.12, F.S., and to deactivate the access permissions of those persons; and
- The ability to utilize the Uniform Port Access Credential Card in a manner that is designed to ensure the credentialed cardholder's privacy in a manner consistent with the state's security requirements.

A fingerprint-based criminal history check shall be performed on an applicant for a Uniform Port Access Credential Card. Based upon review of the criminal history check, each seaport may determine the specific access permissions that will be granted to that applicant.

III. Effect of Proposed Changes:

This bill creates s. 311.125 (15), F.S., to authorize the Department of Highway Safety and Motor Vehicles to designate the TSA TWIC card as the Uniform Port Access Credential Card. The effect of this bill is to establish a single uniform access credential card for use at Florida's public seaports. This bill applies only to the provisions of s.311.125, F.S., and does not affect other provisions of Chapter 311, F.S.

The department is authorized to set and collect a fee for entering a TWIC cardholder into the Uniform Port Access Credential System. Such fee may not exceed the actual cost to the department.

The bill provides that the act shall take effect on becoming a law.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

Issuance of a TWIC card will include fees in order to cover the cost of card stock as well as administration, operation, and maintenance of the required technology, equipment, database systems, and fingerprint-based criminal background checks necessary to operate the TWIC system The TSA is currently implementing TWIC at selected Florida seaports and is currently charging issuing fees.

B. Private Sector Impact:

Each TWIC cardholder or the cardholder's employer will bear the cost of the fees associated with the issuance of a TWIC card. The Governor's Office of Drug Control estimates the individual fees for each card at $132.50 plus an additional administrative maintenance fee (See Government Sector Impact).

C. Government Sector Impact:

Cost to the Department of Highway Safety and Motor Vehicles will be offset by the collection of a fee not to exceed actual cost to the department. At this point, the department estimates the cost to be $30 per card.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Additional Information:

A. Committee Substitute – Statement of Substantial Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.