SENATE STAFF ANALYSIS AND ECONOMIC IMPACT STATEMENT

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

BILL: CS/CS/SB 1616

SPONSOR: Appropriations Subcommittee on Transportation and Economic Development, Committee on Home Defense, Public Security, and Ports and Senator Dockery

SUBJECT: Seaport Security Standards

DATE: April 22, 2003 REVISED: _____ _____ _____ _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Dodson	Skelton	HP	Favorable/CS
2.	Mannelli	Kelly	ATD	Fav/CS
3.			AP	Withdrawn: Fav/CS
4.				
5.				
6.				

I. Summary:

The Committee Substitute for Committee Substitute for SB 1616 revises provisions relating to seaport security standards and provides for the development and implementation of a Uniform Port Access Credentialing System for use by all ports subject to the statewide minimum seaport security standards.

The bill amends s. 311.12, F.S., and creates s. 311.125, F.S.

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 United States. The Maritime Transportation Security Act of 2002 (MTSA)[1] was signed into law by President Bush on November 25, 2002. MTSA authorizes more security officers, more screening equipment, and the building of security infrastructure at the nation's seaports. The law establishes a grant program to make allocations among port authorities, waterfront facility operators, and state and local agencies for the purpose of providing security infrastructure and services.

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. An individual may be denied a card if that person has been convicted within the preceding 7-year period of a felony or found not guilty by reason of insanity of a felony that the Secretary (of the U.S. Department of Transportation) believes could be a terrorism security risk. An individual who has been released from incarceration within the preceding 5-year period for any such felony is ineligible for a transportation security card. A person who may be denied admission to the U.S. or removed from the U.S. under the Immigration and Nationality Act may be denied a card.

The Transportation Security Administration (TSA) is currently establishing a standardized Transportation Worker Identification Credential (TWIC) system consisting of an electronic personal card that will positively identify transportation workers who require unescorted physical and logical access to secure areas and functions of the transportation system. The objective of the TWIC is to provide one standardized, common credential supported by a single integrated and secure network of databases to manage worker access into secure transportation areas and operations.[2]

The Department of Transportation must prescribe regulations that establish a waiver process for issuing a transportation security card to individuals found to be ineligible, and an appeals process is provided for ineligible individuals that includes notice and an opportunity for a hearing.

The Maritime Transportation Security Act directs the Coast Guard to issue regulations to implement the Port Security section of the Act. The Coast Guard plans to publish a temporary interim rule no later than June 2003 and a final rule by November 2003.[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]

---

[2] Broad Agency Announcement (BAA No. DTRS56-02-BAA-0005), U.S. Transportation Security Administration, June 24, 2002.
[3] 67 Fed. Reg. 250 (December 30, 2002) p. 79744
[4] Chapter 2000-360, Laws of Florida.

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.

The statewide standards are set forth in the "Port Security Standards - Compliance Plan" (Compliance Plan) provided to the Legislature on December 11, 2000. Each seaport must maintain a security plan that is tailored to meet the individual needs of the port and assures compliance with the statewide standards. As part of such security plan, a seaport may designate restricted access areas within the seaport.[5] These restricted areas include those areas required by federal law to be "restricted" or "secure" areas, and any other areas selected by a seaport for designation as a restricted area.

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 five 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:

- Dealing in stolen property;
- Trafficking in cannabis;
- Any violation involving the sale, manufacturing, delivery, or possession with intent to sell, manufacture, or deliver a controlled substance;
- Burglary;
- Robbery;
- Display, use, threaten, 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.[6]

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

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 incarceration (and any post incarceration supervision), the person remains free from any subsequent conviction for such offenses for a period of at least 5 years prior to the employment or access date under consideration.

Restricted Access Area Permit/Identification Badges**:** Individuals working within or authorized to regularly enter a restricted access area must have a Restricted Access Area Permit.[7] The Compliance Plan requires all personnel permanently employed at a seaport, including port management staff, tenant activity staff, truckers, stevedores, and longshoremen, to display a picture identification (ID) badge or card at all times when accessing or working within areas as designated by port management. At a minimum, restricted areas include: cargo storage or staging yards; docks/berths; fuel storage or transfer yards; and cruise terminals. Issuance of ID badges by Port Management is contingent on the successful completion of state and federal criminal history checks. The ID badge requirement also applies to day workers and casual laborers who work at the port any more frequently than five days in any given 90 day period.

There currently are no statutory requirements with respect to the type of Restricted Access Area Permit (identification badge) issued. The Compliance Plan requires that picture IDs must be color coded or otherwise identified by hologram or symbol to indicate specific areas to which access is authorized. Lost or stolen cards must be reported and a log maintained of all currently issued and restricted cards. ID badges or cards must be renewed on an annual basis.[8]

To ensure that each seaport had the capability to conduct a background check and issue a Restricted Access Area Permit, the Department of Law Enforcement and the Florida Seaports purchased electronic fingerprint equipment and badging equipment for those seaports issuing the permits. The initial equipment is "stand-alone" computer technology that allows for a badge to be issued on a standard plastic card, or on a "proximity" technology badge that may be "read" by a computer operating system.

To date, only the Port of Miami is currently processing its identification badges through technological means. Individuals seeking access through the main gate at the Port of Miami are given a "proximity card" which is then "read" by a computer operating system with relevant data stored locally on a central network operating center. Information about the individual, including a picture of the individual, is stored in the system. When the card is presented and "read" at the main gate, the individual's information is posted on a computer screen and checked by security personnel to ensure that the individual is authorized to enter the restricted access area.[9]

Appeal Procedure/Waivers: Each seaport security plan may establish a procedure to appeal a denial of employment or access based upon criminal history factors in s.311.12(3)(c), F.S. The appeal procedure may allow the granting of waivers or conditional employment or access. Additionally, a seaport may allow waivers on a temporary basis to meet special or emergency

[7] *Id.*
[8] Standard 1.h., "Port Security Standards – Compliance Plan."
[9] "Credentials/Identification Cards," provided by the Florida Ports Council on January 30, 2003.

needs of the seaport or its users. Policies, procedures, and criteria for implementation of the appeals process must be included in each plan.[10]

Visitor Access: Each seaport security plan must establish conditions and restrictions for persons visiting a port or restricted access area.[11] Visitors are authorized access only to areas specific to their port business and passes are used to convey this permit. Access to a seaport requires checking and recording a visitor's name, purpose of visit, destination, vehicle tag number, and date and time of entry/departure. Visitors are not allowed on the dock or in restricted areas and all vehicles must park in designated areas.[12]

Access Gates and Gate Houses: Seaport gates and gatehouses control access to restricted areas as determined by Port Management. Gates must be located at all perimeter access points and principal interior access points. Gates and gate houses are required to be staffed or locked at all times. Gatehouses at all vehicle entrances and exits must be staffed during business hours unless controlled by electronic access systems, and gatehouses must be situated so that exiting vehicles may be stopped and examined on seaport property.[13]

Designated Parking: Parking within the seaport is restricted, and is authorized by a gate pass and/or decal system. 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. Parking for vehicles authorized on port grounds is restricted to port authority, carrier, maintenance, commercial, and government vehicles essential to seaport operation.[14]

III. Effect of Proposed Changes:

Section 1: This section of CS/CS/SB 1616 amends Section 311.12, F.S., to authorize the Department of Law Enforcement to exempt any public port that has no maritime activity from the statewide minimum seaport security standards. The department must periodically review exempt seaports to determine if there is maritime activity at the seaport. A seaport's change in status from inactive to active may warrant removal of all or part of such exemption.

Section 311.12(2), F.S., is amended to change the term "Restricted Access Area Permit" to "Port Access Credential Card" to conform to provisions made in Section 2 of the bill.

Each seaport security plan may establish a procedure to appeal a denial of employment or access based on procedural inaccuracies or discrepancies regarding criminal history factors. The bill removes current provisions that allow the granting of waivers or conditional employment access based on criminal history factors. The Department of Law Enforcement may authorize waivers on a temporary basis as necessary to meet special or emergency needs of a seaport or its users.

Section 311.12(3)(c), F.S., is amended to add additional offenses that prohibit an individual from gaining initial employment on a seaport or being granted access to restricted areas within the

[10] s. 311.12(3)(b), F.S.
[11] s. 311.12(2), F.S.
[12] Standard 3, "Port Security Standards – Compliance Plan."
[13] Standard 4, "Port Security Standards – Compliance Plan."
[14] Standard 5, "Port Security Standards – Compliance Plan."

seaport. Under provisions of the bill, the following offenses preclude an individual from working on or accessing secure areas of a seaport are added:

- A forcible felony as defined in s. 776.08, F.S.
- An act of terrorism as defined in s. 775.30, F.S.
- Planting of a hoax bomb as provided in s. 790.165, F.S.
- Manufacture, possess, sale, delivery, display, use, or attempted or threatened use of a weapon of mass destruction or hoax weapon of mass destruction as provided in s. 790.166, F.S.

Under current law, seaports may implement security measures that are more stringent, greater than, or supplemental to the statewide minimum standards.[15] CS/CS/SB 1616 revises this provision to require seaports to adhere to the offense criteria and other provisions of s. 311.12(3)(c), F.S. For purposes of employment and access, the bill prohibits a seaport from exceeding the statewide minimum requirements.

Section 2: A new section 311.125, F.S., is created to provide for the implementation of a Uniform Port Access Credential System. By July 1, 2004, each seaport subject to the statewide minimum seaport security standards must use a Uniform Port Access Credential Card that is accepted at all identified seaports. Each seaport is responsible for operating and maintaining the system to control access security within the boundaries of the seaport.

The Department of Highway Safety and Motor Vehicles (DHSMV) will administer the system and will issue credential cards to the designated port authority or recognized governing board of each seaport for distribution to credential applicants.

DHSMV must consult with the Department of Law Enforcement and the U.S. Transportation Security Administration (TSA) to develop the system. The system will be used to issue credentials to all persons working on a seaport and must be designed to conform, as closely as possible, to the criteria established by the TSA for a Transportation Worker Identification Card or other federal identification required by law.

The bill provides specific requirements for the Uniform Port Access Credential System to address collection and storage of fingerprints and other biometric identifiers and a methodology for granting access permissions and deactivating the permissions of credential holders who have violated access requirements.

CS/CS/SB 1616 also provides minimum requirements including photographs, fingerprints, barcodes, scanning capability, and color differentials to be used for the Uniform Port Access Credential Card.

A fingerprint-based criminal history check will be performed on each credential applicant and each seaport will use such checks to determine the specific access permissions to be granted to each applicant. After determining that an applicant is eligible, a seaport must provide DHSMV an authorization form and a copy of the applicant's criminal history check results. The

[15] S. 311.12(5), F.S.

department will then issue the credential card to the port authority to be distributed to the card applicant.

A credential card is valid for a period of four years and random criminal history checks may be performed during that period. Access will be denied to any applicant who fails to complete any part of the credential application process or who does not comply with criminal history requirements. Access authority may be restricted or revoked: if a cardholder is suspected of criminal violations that could affect the security of a port; upon suspicion that the person is using or attempting to use the card fraudulently; or if restriction or revocation is done to assure the security of a port.

A law enforcement officer may seize a Uniform Port Access Credential Card if he has reasonable suspicion to believe that a card is possessed or is being used in violation of law or the standards provided for credentials. A cardholder has no cause of action against a law enforcement officer who seizes a Uniform Port Access Credential Card.

The bill provides a process for a credential card to be placed in an inactive status and to be reactivated by petition. Corporations, individuals, or other business entities that employ persons who work on or conduct business at a seaport must notify those seaports accessed by their employees in the event of a separation from employment. If a business fails to report an employee's work status change within 7 days, the business' seaport access may be revoked.

A credential card must contain biometric verification of a cardholder's identity and proper access permissions. To gain entrance to a restricted area, a machine check and fingerprint verification of a credential card is required. For those seaports with restricted access areas adjacent to nonrestricted areas, secondary machine checks and fingerprint verification of credentials are required at restricted area entrances. When a person exits a gated area of a seaport, a machine check of his or her credential card is required.

The bill contains provisions regarding access to restricted areas of seaports. A person must stop at a check point and present valid identification to receive a visitor's pass before proceeding. Buses entering seaports must be able to verify that all passengers have legitimate business on the port. Failure to display a visitor's pass will result in revocation of a person's permission to access a seaport.

The price of a Uniform Port Access Credential Card will be set by DHSMV to include the costs of initial state and federal criminal history checks, annual criminal history checks, and production costs. Seaports are allowed to charge an additional administrative fee not to exceed $25 per card for costs associated with issuing the credentials.

The bill provides implementation dates for the Uniform Port Access Credential System. Seaports must comply with technology improvement requirements necessary to activate the Uniform Port Access Credential System no later than July 1, 2004. DHSMV must specify equipment and technology requirements no later than July 1, 2003. The system must be implemented at the earliest possible time that all ports have active technology in place, but no later than July 1, 2004.

The provisions of this section are contingent upon the receipt of federal grant funds necessary to implement the Uniform Port Access Credential System.

Section 3: The bill takes effect upon becoming a law.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. Other Constitutional Issues:

None.

V. Economic Impact and Fiscal Note:

A. Tax/Fee Issues:

Individual ports now charge issuance fees for port access identification cards. Under the provisions of CS/CS/SB 1616, these fees would be collected by DHSMV.

B. Private Sector Impact:

An issuance fee would continue to be charged for processing of criminal history checks and card production. The price would be determined based on the costs associated with initial and annual criminal history checks and production expenses.

C. Government Sector Impact:

The Department of Highway Safety and Motor Vehicles would be responsible for determining the cost of the Uniform Port Access Credential System. Preliminary estimates are that this will cost approximately $2.0 million in the first year and $584,000 annually thereafter for operations and maintenance costs.

The Senate General Appropriations Act for FY 2003-04, SB 2500, includes $20.0 million from the federal government for unrelated security improvements. Federal funding for the security improvements necessitated by the Uniform Port Access Credential System will become available from the supplemental Congressional appropriation for the Iraq War and implementation is contingent on the receipt of federal grant funds.

The annual recurring costs will be supported by fees paid by those receiving the credential cards.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Amendments:

None.

This Senate staff analysis does not reflect the intent or official position of the bill's sponsor or the Florida Senate.