

**FLORIDA SEAPORT TRANSPORTATION AND
ECONOMIC DEVELOPMENT COUNCIL
SECURITY COMMITTEE MEETING**

TUESDAY, JUNE 7, 2005

JACKSONVILLE, FLORIDA

TAB 1

CALL TO ORDER

A G E N D A

MEETING: FSTED COUNCIL SECURITY COMMITTEE MEETING

DATE: Tuesday, June 7, 2005

TIME: 10:00 a.m. – 3:00 p.m.

PLACE: JaxPort Boardroom

1. Call to Order.
2. Roll Call.
3. Discussion of 2005 Regular Legislative Session Issues.
 - A. Seaport Security Officer Legislation.
 - B. Other Seaport Security Issues.
4. Review of Seaport Security Measure Infrastructure Project Requests.
5. Discussion of FDLE Inspection Activity and Waivers
 - A. FDLE Written Guidelines.
 - B. Status of Current Seaport Security Inspections.
 - C. Section 311.12(4)(e), F.S. – November 2005 Legislative Review of Non-compliant Seaports.
6. Discussion of Federal FY 2005 Port Security Grant Program.
7. Review of Status of Florida Uniform Port Access/TWIC Card.
8. Discussion of Caribbean Basin Maritime Security Issues.
9. Other Issues.
10. Adjournment.

TAB 2

ROLL CALL

ROLL CALL

MEMBER:

DESIGNEE:

CANAVERAL

EVERGLADES

FERNANDINA

FT. PIERCE

JACKSONVILLE

KEY WEST

MANATEE

MIAMI-DADE

PALM BEACH

PANAMA CITY

PENSACOLA

PORT ST. JOE

ST. PETERSBURG

TAMPA

TAB 3

DISCUSSION OF 2005 REGULAR SESSION ISSUES



502 East Jefferson Street, Tallahassee, Florida 32301

Telephone: (850) 222-8028

Fax: (850) 222-7552

www.flaports.org - E-Mail: info@flaports.org

MEMORANDUM

DATE: May 9, 2005
TO: Florida Port Directors
FROM: Michael L. Rubin
SUBJECT: **END OF SESSION LEGISLATIVE REPORT**

The Florida Legislature completed its work 10 minutes before midnight on Friday, May 6, 2005. We provide the following report on bills that passed the Legislature and on bills that did not pass this Session:

I. Bills That Passed During Regular Session 2005.

1. Fiscal Year 2005/06 General Appropriations Act. The Fiscal Year 2005/06 General Appropriations Act (GAA) was passed by the Full Legislature on Friday, May 6, 2005. The FY 2005/06 Appropriations Act provides the following appropriations for seaport issues:

- A. Specific Appropriation 1993 – \$15 million for 1996 FPFC Bonds Debt Service Payment Funds.
- B. Specific Appropriation 1994 – \$10 million for 1999 FPFC Intermodal Program Bonds Debt Service Payment Funds.
- C. Specific Appropriation 1995 – \$33,183,000 for FSTED Program Funds. This line item provides \$10 million for Chapter 311 projects, \$5 million for Chapter 311 intermodal projects, \$13,183,000 for SIS intermodal hub and connector projects, and \$5 million for small county dredging projects.

The \$5 million for small county dredging projects is contingent upon the Governor's approval of HB 1029 or HB 1681 which passed the Legislature authorizing the creation of a small county dredging program by the FSTED Council, and his approval of the GAA Implementing Bill's language related to this issue.

- D. Specific Appropriation 2090A – \$1.2 million to HSMV for card readers/biometric technology for the seaport UPAC/TWIC system.

2. SB 360/HB 1865 – Relating to Growth Management. The House and Senate met in Conference on Friday, May 6, 2005, and crafted a consensus bill on Growth Management regulation and funding. The bill contains various provisions for growth management regulations, concurrency requirements, and transportation funding. The bill contains \$575 million for transportation projects in Fiscal Year 2005/06 for the following purposes:

A. \$275 million for projects identified pursuant to the newly created Transportation Regional Incentive Program (TRIP). SB 360 created the TRIP program within the Department of Transportation to “provide funds to improve regionally significant transportation facilities.” Under this program, the FDOT is to allocate funds to its districts for projects that, at a minimum, provide the following:

1. Support transportation facilities that serve national, statewide, or regional functions and function as an integrated regional transportation system.
2. Are identified in the capital improvements element of a comprehensive plan that is in compliance with growth management regulations. The project must also be in compliance with comprehensive plan policies relative to corridor management.
3. Are consistent with the SIS plan.
4. Have a commitment for local, regional, or private financial matching funds as a percentage of the overall project cost. (Note: The TRIP program requires a 50 % match of funds provided.)

B. \$200 million for projects identified pursuant to the SIS plan.

C. \$100 million for projects identified pursuant to the State-funded Infrastructure Bank.

These funds were appropriated in the bill on a non-recurring basis. However, the bill amends statutory language concerning Documentary Stamp fees assessed on real estate transactions, and designates that a portion of those fees shall be used as a recurring source of funding for such transportation projects.

We would note that the statutory changes to growth management laws were extensive, and we will provide additional information on this bill as they are reviewed and implemented by the appropriate state agencies.

3. SB 1576/HB 1029 – Relating to Dredging Projects. HB 1029 was passed by the Full Legislature on April 28, 2006. The bill has not been presented to the Governor to date. The language authorizing the creation of the program also was passed in the Appropriations Implementing Bill and HB 1681 (relating to transportation).

4. SB 1414/HB 1715 – Relating to the Domestic Security Oversight Board. HB 1715 was passed

by the Full Legislature on May 4, 2005. The bill revises laws relating to the make-up and authority of the Domestic Security Oversight Board. The Board reviews State domestic security policies and makes recommendations on the allocation of federal security dollars to entities state-wide. With respect to seaports, the bill provides that the FSTED Council now is a voting member of the Board.

5. SB 288/HB 1691 – Relating to Public Records Exemption for Seaport Security Plans. SB 288 was passed by the Full Legislature on May 4, 2005. The bill extends the public records exemption for seaport security plans.
6. SB 1670/HB 1627 – Relating to Oceans and Coastal Resources Act. The bill language creating the Oceans and Coastal Resources Act was amended on to HB 1855 (relating to natural resources) and passed by the Full Legislature on May 6, 2005. The bill creates the Florida Oceans and Coastal Council within the Florida Department of Environmental Protection. The Council is responsible for developing a “research plan” by January 15, 2006, that includes among other requirements the compilation of existing and new oceans and coastal research, as well as “exploring opportunities to improve coastal ecosystem functioning and health through watershed approaches to managing freshwater and improving water quality.” Of the fifteen members of the Council, the Florida Ocean Alliance shall present the Commissioner of the Department Agriculture and Consumer Services with at least eight names from which to choose five members.

II. Bills That Did Not Pass During Regular Session 2005.

1. SB 1062/HB 1799 – Relating to Seaport Security Officers. The Full Senate passed SB 1062 by a unanimous vote of 39 yeas to 0 nays on May 5, 2005. In addition to creating a certification process for “seaport security officers,” the Senate bill also included specific legislative intent that operational efficiencies be developed on seaports, and that certified seaport security officers could be used in lieu of badged law enforcement officers to the maximum extent feasible.

A similar House bill died in the Fiscal Council.

2. Legalized Gambling – Slot Machine Discussions. The House and Senate failed to reach consensus on slot machine regulations for Broward County pari-mutuel facilities. We would note the issue of taxes upon cruise vessels did not appear on either the House or Senate bills as they moved through the process.

If you have any questions, please call us at (850) 222-8028.

mlr/njl

N:\2005 Session\Legislative Report - End of Session 2005.wpd

TAB 3A

SEAPORT SECURITY OFFICER LEGISLATION

1 A bill to be entitled
2 An act relating to seaport security; amending
3 s. 311.12, F.S.; requiring that the Department
4 of Law Enforcement establish a waiver process
5 for allowing an individual, who is otherwise
6 unqualified, to be allowed unescorted access to
7 a seaport or restricted access area; requiring
8 that the administrative staff of the Parole
9 Commission review the facts of the waiver
10 application and transmit the findings to the
11 Department of Law Enforcement; requiring the
12 department to make a final disposition of the
13 application and notify the applicant and the
14 port authority that denied employment to the
15 applicant; exempting the review from ch. 120,
16 F.S.; creating s. 311.121, F.S.; authorizing
17 the seaport authority or governing board of
18 certain seaports to require that seaport
19 security officers receive additional training
20 and certification; providing legislative intent
21 relating to mitigation of operational security
22 costs at seaports; requiring the department to
23 apply such intent; providing eligibility
24 requirements for such certification; creating
25 the Seaport Security Officer Qualifications,
26 Training, and Standards Steering Committee to
27 develop the curriculum for the training
28 program; providing for the membership of the
29 steering committee; requiring the Department of
30 Education to implement the training curriculum;
31 authorizing the substitution of training

1 equivalencies; requiring an examination;
2 providing requirements for certification
3 renewal; providing continuing education
4 requirements for certification; providing
5 requirements for schools that offer training
6 for seaport security officers; providing for
7 issuance of a license indicating that the
8 licensee is certified as a seaport security
9 officer; creating s. 311.122, F.S.; authorizing
10 a seaport security officer to take into custody
11 any person whom the officer has cause to
12 believe is trespassing in a restricted access
13 area; providing that such officer is not
14 criminally or civilly liable for taking such
15 action; defining the term "restricted access
16 area"; providing for designation of part or all
17 of a seaport as a restricted access area under
18 certain emergency conditions; creating s.
19 311.123, F.S.; requiring that the Florida
20 Seaport Transportation and Economic Development
21 Council, in conjunction with the Department of
22 Law Enforcement and the Governor's Office of
23 Drug Control, create a maritime domain
24 awareness training program; providing purposes
25 of the program; providing requirements for the
26 curriculum; providing an effective date.

27
28 Be It Enacted by the Legislature of the State of Florida:
29

30 Section 1. Paragraph (e) is added to subsection (3) of
31 section 311.12, Florida Statutes, to read:

1 311.12 Seaport security standards.--
2 (3)
3 (e) The Department of Law Enforcement shall establish
4 a waiver process for allowing unescorted access to an
5 individual who is found to be unqualified under paragraph (c)
6 and denied employment by a seaport. The waiver consideration
7 shall be based on the circumstances of any disqualifying act
8 or offense, restitution made by the individual, and other
9 factors from which it may be determined that the individual
10 does not pose a risk of engaging in theft, drug trafficking,
11 or terrorism within the public seaports regulated under this
12 chapter or of harming the residents of this state. The waiver
13 process shall begin when an individual who has been denied
14 initial employment within or regular unescorted access to
15 restricted areas on a public seaport as described in paragraph
16 (c) submits an application for a waiver, along with a
17 notarized letter or affidavit from the individual's employer
18 or union representative, which states the mitigating reasons
19 for initiating the waiver process. No later than 90 days after
20 receipt of the application, the administrative staff of the
21 Parole Commission shall conduct a factual review of the waiver
22 application. Findings of fact shall be transmitted to the
23 Department of Law Enforcement for review. The department shall
24 make a copy of those findings available to the applicant
25 before final disposition of the waiver request. The department
26 shall make a final disposition of the waiver request based on
27 the factual findings of the investigation by the Parole
28 Commission. The port authority that originally denied
29 employment and the waiver applicant shall be notified of the
30 final disposition of the waiver application by the department.
31 This review process is exempt from chapter 120.

1 Section 2. Section 311.121, Florida Statutes, is
2 created to read:

3 311.121 Qualifications, training, and certification of
4 licensed security officers working on Florida seaports.--

5 (1) Each seaport authority or governing board of a
6 seaport identified in s. 311.09 which is subject to the
7 statewide minimum seaport security standards set forth in s.
8 311.12 may require that security officers working on the
9 seaport receive additional training and certification as a
10 seaport security officer. In accordance with s. 311.12(4), it
11 is the intent of the Legislature to provide seaports in this
12 state with the ability to mitigate operational security costs
13 without reducing security through a combination of sworn law
14 enforcement officers and certified private security services
15 as provided in this section. To the maximum extent feasible,
16 the Florida Department of Law Enforcement shall apply this
17 intent in achieving the security requirements as required in
18 s. 311.12.

19 (2) Any person who has received a Class D license as a
20 security officer pursuant to chapter 493 and successfully
21 completed the entire certified training curriculum for a Class
22 D license, or who has been determined to have equivalent
23 experience by the Department of Agriculture and Consumer
24 Services, is eligible to complete training and testing to
25 become certified as a seaport security officer. As used in
26 this subsection, the term "equivalent experience" means
27 experience that is substantially identical and equal in force,
28 power, and effect or import as the experience gained by
29 personal knowledge and activity for the required period of
30 time performing the type of service permitted under the
31 license for which application is made. The department shall

1 have final authority over any determination of equivalent
2 experience.

3 (3) The curriculum for the seaport security officer
4 training program shall be developed by the Seaport Security
5 Officer Qualifications, Training, and Standards Steering
6 Committee. The curriculum must require no less than 8 hours
7 of initial certification training and must conform to or
8 exceed the model courses for facility personnel with specific
9 security duties which have been approved by the federal
10 Maritime Administration under Section 109 of the federal
11 Maritime Transportation Security Act of 2002. The steering
12 committee shall meet at least once each year to update or
13 modify the curriculum. Members of the Steering Committee shall
14 be appointed by the Department of Law Enforcement. Members
15 shall serve for the duration of their employment or
16 appointment in a specified position, or for a term of 4 years
17 if not designated by title to a specified position. The
18 members of the steering committee shall be the Seaport
19 Administrator of the Department of Law Enforcement, the
20 Chancellor of the Community College System, the Director of
21 the Division of Licensing of the Department of Agriculture and
22 Consumer Services, the Administrator of the Florida Seaport
23 Transportation and Economic Development Council, two seaport
24 security directors from ports designated in s. 311.09, one
25 director of a state law enforcement academy, one
26 representative of a local law enforcement agency, two
27 representatives of contract security services, one
28 representative of the Division of Driver Licenses of the
29 Department of Highway Safety and Motor Vehicles, and one
30 representative of the United States Coast Guard.

31

1 (4) The Department of Education shall be responsible
2 for implementing the curriculum recommendations of the Seaport
3 Security Officer Qualifications, Training, and Standards
4 Steering Committee in order to provide a training program for
5 certified seaport security officers which shall be used by
6 licensed schools pursuant to s. 493.6304. Each instructor
7 providing training must hold a Class DI license pursuant to s.
8 493.6301. A seaport authority or other organization involved
9 in seaport-related activities may apply to become a licensed
10 school pursuant to s. 493.6304.

11 (5) The Seaport Security Officer Qualifications,
12 Training, and Standards Steering Committee may consider
13 training equivalencies that may be substituted for the
14 required training. These equivalencies must be established and
15 made known to persons seeking certification in advance of
16 training. A candidate for certification as a seaport security
17 officer shall be required to successfully pass a proficiency
18 examination.

19 (6) Persons who successfully complete the training, or
20 training equivalency, and pass the examination shall receive a
21 State of Florida Seaport Security Officer Certificate. This
22 certificate authorizes the bearer to represent that he or she
23 is qualified to perform duties specifically required of a
24 seaport security officer. The certificate shall remain valid
25 for the duration of an active Class D license and shall be
26 considered renewed upon proper renewal of the Class D license.
27 The certificate becomes void if the Class D license is revoked
28 or allowed to lapse for more than 1 year. Renewal of
29 certification following revocation or a lapse of longer than 1
30 year of a Class D license requires, at a minimum,
31 reexamination of the applicant.

1 (7) The steering committee shall recommend a
2 continuing education curriculum to be implemented by the
3 Department of Education. The curriculum must be offered by
4 any licensed school or seaport that offers certificate
5 training for seaport security officers and must require no
6 less than 4 hours of additional training per annual licensing
7 period. A seaport security officer certificate is void if the
8 certificateholder licensee fails to complete the annual
9 continuing education requirement prior to expiration of his or
10 her Class D license.

11 (8) A State of Florida Seaport Security Officer
12 Certificate may be issued by a school licensed pursuant to s.
13 493.6304 upon a person's successful completion of the training
14 curriculum, proof of any applicable training equivalencies,
15 and passage of a proficiency examination. The certificate
16 shall be provided by the Department of Agriculture and
17 Consumer Services for issuance by the school. A school shall
18 notify the Division of Licensing within the department upon
19 the issuance of each State of Florida Seaport Security Officer
20 Certificate. The notification must include the name and Class
21 D license number of the certificateholder and a copy of the
22 certificate. The department shall place the notification with
23 the Class D licensee's file. Notification may be made through
24 an electronic or paper format pursuant to instructions of the
25 Department of Agriculture and Consumer Services.

26 (9) Upon completion of the certification process, a
27 person holding a Class D license shall be required to apply
28 for a revised duplicate license pursuant to s. 493.6107(2).
29 The revised duplicate license must contain language or
30 markings indicating that the licensee is certified as a
31 seaport security officer.

1 Section 3. Section 311.122, Florida Statutes, is
2 created to read:

3 311.122 Trespassing; detention by a certified seaport
4 security officer.--Any Facility Security Officer as designated
5 pursuant to 33 C.F.R. part 105 for each seaport identified in
6 s. 311.09, or any employee or agent holding a Class D or Class
7 G license and certification as a seaport security officer who
8 is designated by the Facility Security Officer to maintain
9 order and provide security within the seaport, who has
10 probable cause to believe that a person is trespassing in a
11 designated restricted access area of a seaport pursuant to s.
12 810.08 or s. 810.09 may take such person into custody and
13 detain him or her in a reasonable manner for a reasonable
14 length of time pending the arrival of a law enforcement
15 officer. Such taking into custody and detention by an
16 authorized person does not render that person criminally or
17 civilly liable for false arrest, false imprisonment, or
18 unlawful detention. If a trespasser is taken into custody, a
19 law enforcement officer shall be called to the scene
20 immediately after the person is taken into custody. For the
21 purposes of this section, the term "designated restricted
22 access area" means an area where signage, fencing, or other
23 access-control measures designed to prevent unauthorized
24 access to that area are in place. During a period of a high
25 terrorist threat level, as defined by the United States
26 Department of Homeland Security or the Department of Law
27 Enforcement, or during a period of emergency declared by the
28 seaport security director of a particular port due to events
29 applicable to that particular port, the management or
30 controlling authority of the port may temporarily designate
31 any part or all of the port property as a restricted access

1 area. The duration of any such temporary designation is
2 limited to the period when the high terrorist threat level or
3 port emergency exists. This section does not limit the power
4 of the managing or controlling authority of a seaport to
5 designate any or all of the port property as a restricted
6 access area as otherwise provided by law.

7 Section 4. Section 311.123, Florida Statutes, is
8 created to read:

9 311.123 Maritime domain awareness training of
10 personnel working on Florida seaports.--The Florida Seaport
11 Transportation and Economic Development Council, in
12 conjunction with the Department of Law Enforcement and the
13 Office of Drug Control within the Executive Office of the
14 Governor, shall create a maritime domain awareness training
15 program. The program shall provide training designed to
16 instruct all workers within a seaport's boundaries about the
17 security awareness procedures required of those workers in
18 order to implement the security plan of the seaport. The
19 training program curriculum must also include security
20 training required pursuant to 33 C.F.R. part 105 and must be
21 designed to enable the seaports in this state to meet the
22 training, drill, and exercise requirements of 33 C.F.R. part
23 105, individual seaport security plans, and the security
24 awareness requirements of s. 311.12.

25 Section 5. This act shall take effect July 1, 2005.
26
27
28
29
30
31

TAB 3B

OTHER SEAPORT SECURITY ISSUES

TAB 4

**REVIEW OF SEAPORT SECURITY MEASURE
INFRASTRUCTURE PROJECT REQUESTS**

TAB 5

**DISCUSSION OF FDLE INSPECTION ACTIVITY
AND WAIVERS**

TAB 5A

FDLE WRITTEN GUIDELINES



Florida Department of
Law Enforcement

Guy M. Tunnell
Commissioner

Post Office Box 1489
Tallahassee, Florida 32302-1489
(850) 410-7001
<http://www.fdle.state.fl.us>

Jeb Bush, *Governor*
Charlie Crist, *Attorney General*
Tom Gallagher, *Chief Financial Officer*
Charles H. Bronson, *Commissioner of Agriculture*

April 19, 2005

Inspection Guidance of Security Activity Compliance

Question: Multiple agencies and private tenants conduct security activities on seaports. During the inspection process how do FDLE inspectors judge compliance with the mandatory F.S. 311.12 security duties? How is the performance by federal, state, and local law enforcement; tenant security employees or contract security firms with contractual relationships with tenants; and seaport agency security employees or contract security firms with contractual relationships with the seaport agency judged as components related to meeting the F.S. 311.12 standards? Can seaport agencies rely on tenants as a way to meet the F.S. 311.12 standards? Can the activities of federal agencies like CPB be the mechanism by which the seaports meet the standards.

Answer: Seaport agencies are the entity required to perform the seaport security activities associated with the standards of F.S. 311.12. It was intended that there would be an additional security layer established under F.S. 311.12.

The Camber Corporation study (September 2000) provided to the legislature by the Office of the Governor on which the legislature based the creation of F.S. 311.12 states: *“Seaport security is influenced by the actions of numerous federal, state, and local agencies (e.g. customs, INS, USCG, DOT, law enforcement, city/county Commissions) over which ports have virtually no control.”*

The Camber Corporation went on to state, *“Given the relatively free movement of goods once they enter the United States, seaports may be considered the last line of defense-in-depth. That being noted, however, it is important to recognize Florida’s fourteen deepwater ports for what they should be, relatively fortified positions along an extensive and highly diversified coastline.”*

The Camber Corporation concluded, *“Notwithstanding advocacy of the view that seaport security should be a shared responsibility, the remainder of this report will focus primarily on the particular responsibility of port management, since they are accountable for operation of their respective facilities. Accordingly, subsequent discussion will be aimed at considering those specific aspects of seaport security for which it is reasonable to expect port management to be held accountable. As a result, however, the report will not address other aspects of security that are more appropriately the purview of the private tenants that operate from our seaports...Rather, it will examine, in detail, those security functions which the State should expect from the managers of its ports and those areas where port management has the greatest opportunity for positively impacting the security posture of their ports against criminal activity and drug smuggling.”*

The result of the Camber Corporation study was their recommendation and the legislature’s adoption of the Florida seaport security standards as those that meet the test of being the **“particular responsibility of port management”**.

From an inspection perspective seaports may achieve compliance related to certain elements of F.S. 311.12 that relate to the performance of security activities by doing the following:

1. Seaports must have a memorandum of understanding with one or more local law enforcement agencies that includes an appropriate level of seaport patrol; officer training in seaport security; officer enforcement of **all** of the elements of the seaport security plan; back up and support for civilian D and G guards performing seaport security functions; and the pre-placement of law enforcement for security support at passenger terminals and/or other restricted access areas during operations where such officers are required to prevent and repel threat against those areas. Alternatively, if authorized by law a seaport agency could have a sworn law enforcement force that was part of the seaport agency. There must be a mechanism in the MOU and monitoring by the seaport agency to ensure that the requirements of the MOU are being met.
2. Seaports may have a memorandum of understanding with a local law enforcement agency that includes the responsibility for the performance of F.S. 311.12 seaport security activities in addition to those in (1) above up to and including all seaports security activities in the plan including FSO activities. Specifically trained sworn and nonsworn employees of the law enforcement agency may conduct these activities. In both (1) and (2) the seaport must have a mechanism to measure and ensure the performance of law enforcement and the MOU.
3. Seaports are not required to use sworn law enforcement personnel for all seaport security activities. Seaports may perform those seaport activities required by F.S. 311.12 with nonsworn personnel when the activities are within the legal use of force authority of individuals that have D or G guard licenses. Port agency employees or security firms that are under contract to the seaport may perform such tasks. All such employees of the seaport or employees of the contractor must have a current D or G guard license. Training must be adequate related to seaport security. Seaports must have a management structure in place to ensure employee performance and/or a contractual mechanism and monitoring to ensure the performance of any security contract firm that has a contractual relationship with the seaport.
4. Seaports may blend the law enforcement activity in (1) above with the civilian activity in (3) above in ways that meet the legal requirements of use of force, pre-place law enforcement for best effect, ensure adequate public safety in the event of threat, and maximize budgetary efficiency.
5. Seaports may NOT delegate to tenants the responsibility to perform the security activities required by F.S. 311.12. However, some security activities that will be performed by tenants overlap the security requirements of the seaport. Two examples follow:
 - a. Example; under USCG requirements and business liability requirements seaport tenants that conduct passenger operations have a responsibility for screening passengers and carry on baggage. The F.S. 311.12 standard requires that seaport management must “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 (as a minimum)”. It is not practical or reasonable to subject passengers to back to back screening within a terminal or restricted access area by the seaport and the tenant. As a consequence, FDLE finds that compliance is attained by the seaport if:
 - i. The seaport agency conducts the passenger screening on behalf of the agency and the tenant with properly trained D or G licensed guards that are employees of the seaport agency, under contract to the seaport agency or employees of the local law enforcement agency in a civilian or sworn capacity under an MOU with the seaport agency.
 - ii. The tenant conducts the passenger screening with properly trained G or D licensed guards at the 100% level that are employees of the tenant or under contract to the

tenant as long as such operation is under the continuous observation and general control of employees of the seaport agency trained to monitor the activity and who have adequate authority to ensure it is being properly performed.

- iii. There is in either event adequate sworn law enforcement presence pre-placed to respond to the presence of weapons and other contraband identified in the screening process.
 - b. Example; tenants in some seaports exercise control over entry into their facilities and/or onto the docks in their particular lease hold. Seaports have a responsibility to maintain access control over entry into all restricted access areas which includes cargo areas and berths/docks. The seaport may not create a seaport access control mechanism by adopting SOPs, constructing gates and roadways and creating designated restricted and non-restricted areas that provide tenants with the only control over access to those areas that are required to be restricted access areas under F.S. 311.12. As in the case of baggage screening (above), the seaport agency security apparatus must either perform the access control task or directly observe and control the performance of the access control task in a way that ensures that the seaport has the ability to deny access to any individual not directly meeting the access control test. The seaport agency may not delegate moment to moment access control to tenants and allow tenants the primary access control into any restricted access area and meet the compliance test.
6. With regard to the other security activities that that occur on seaports that are initiated by federal, state and local partners. Seaports must develop executive security committees that include federal, state, and local law enforcement partners to coordinate security and protection of the seaport. However, seaports cannot step away from an active seaport security layer and performance as a result of the efforts of these agencies. The Camber Corporation study was clearly designed to identify a new model for security on the landlord tenant public seaports in Florida and there is a specific requirement that the seaport management is the responsible entity for the standards.

Conclusion: When inspecting security activities to determine seaport agency compliance, FDLE inspectors look for a seaport agency security layer that is under the control and direction of the seaport agency. Because significant elements in the original legislation that established F.S. 311.12 included public safety beyond the boundary of the seaport and included the interruption of internal drug smuggling conspiracies by those with seaport operations and access it must be the seaport agency that controls or conducts the F.S. 311.12 elements. Since the passage of the legislation, the issue of terrorism has surfaced as a greater concern than originally identified in the Camber Study. This emerging public policy issue increases the general public safety responsibility for the life, health and economic well being for those beyond the boundary of the seaport, for those workers on the seaport, and for those passengers who enter into a place they know is under the control of a government agency. This places a greater burden on ALL public agencies that operate critical infrastructure. As a consequence the issues associated with increased threats from terrorists further strengthen the need for a seaport agency security layer that meets the F.S. 311.12 standard.

Seaports that are meeting their obligation to the legislature to come into compliance with the standards are less at risk from a terrorist attack; better able to limit crime including cargo theft; and performing the public safety service of interdicting the flow of illegal drugs. Seaports and seaport agency managers, as specified in the Camber Study, that fail to meet the compliance test are not meeting those obligations.

TAB 5B

**STATUS OF CURRENT SEAPORT SECURITY
INSPECTIONS**

TAB 5C

**SECTION 311.12(4)(C), F.S. – NOVEMBER 2005
LEGISLATIVE REVIEW OF NON-COMPLIANT
SEAPORTS**

Select Year:

The 2004 Florida Statutes

[Title XXII](#)
PORTS AND
HARBORS

[Chapter 311](#)
FLORIDA SEAPORT TRANSPORTATION AND
ECONOMIC DEVELOPMENT

[View Entire
Chapter](#)

311.12 Seaport security standards.--

(1)(a) The statewide minimum standards for seaport security for each seaport identified in s. [311.09](#) shall be those based upon 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, pursuant to this section. The statewide minimum standards are hereby adopted. The Office of Drug Control within the Executive Office of the Governor shall maintain a sufficient number of copies of the standards for use of the public, at its offices, and shall provide copies to each affected seaport upon request.

(b) The Department of Law Enforcement may exempt any seaport identified in s. [311.09](#) from all or part of the requirements of subsections (1)-(5) if the department determines that the seaport is not active. The department shall periodically review exempted seaports to determine if there is maritime activity at the seaport. A change in status from inactive to active may warrant removal of all or part of any exemption provided by the department.

(2) Each seaport identified in s. [311.09](#) shall maintain a security plan relating to the specific and identifiable needs of the seaport which assures that the seaport is in substantial compliance with the statewide minimum standards established pursuant to subsection (1). Each plan adopted or revised pursuant to this subsection must be reviewed and approved by the Office of Drug Control and the Department of Law Enforcement. All such seaports shall allow unimpeded access by the Department of Law Enforcement to the affected facilities for purposes of inspections or other operations authorized by this section. Each seaport security plan may establish restricted access areas within the seaport consistent with the requirements of the statewide minimum standards. In such cases, a Uniform Port Access Credential Card, authorizing restricted-area access, shall be required for any individual working within or authorized to regularly enter a restricted access area and the requirements in subsection (3) relating to criminal history checks and employment restrictions shall be applicable only to employees or other persons working within or authorized to regularly enter a restricted access area. Every seaport security plan shall set forth the conditions and restrictions to be imposed upon others visiting the port or any restricted access area sufficient to provide substantial compliance with the statewide minimum standards.

(3)(a) A fingerprint-based criminal history check shall be performed on any applicant for employment, every current employee, and other persons as designated pursuant to the seaport security plan for each seaport. The criminal history check shall be performed in connection with employment within 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 or at other more frequent intervals as provided by the seaport security plan. Each individual subject to the background criminal history check shall file a complete set of fingerprints taken in a manner required by the Department of Law Enforcement and the seaport security plan. Fingerprints shall be submitted to the Department of Law Enforcement for state processing and to

the Federal Bureau of Investigation for federal processing. The results of each fingerprint-based check shall be reported to the requesting seaport. The costs of the checks, consistent with s. [943.053\(3\)](#), shall be paid by the seaport or other employing entity or by the person checked.

(b) By January 1, 2002, each seaport security plan shall identify criminal convictions or other criminal history factors consistent with paragraph (c) 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 access area on or after January 1, 2002, and may be used to disqualify all those employed or authorized for regular access on that date. Each seaport security plan may establish a procedure to appeal a denial of employment or access based upon procedural inaccuracies or discrepancies regarding criminal history factors established pursuant to this paragraph. 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 this subsection shall be included in the seaport security plan. All waivers granted pursuant to this paragraph must be reported to the Department of Law Enforcement within 30 days of issuance.

(c) In addition to other requirements for employment or access established by each seaport pursuant to its seaport security plan, each seaport security plan shall provide that:

1. Any person who has within the past 7 years been convicted, regardless of whether adjudication was withheld, for a forcible felony as defined in s. [776.08](#); an act of terrorism as defined in s. [775.30](#); planting of a hoax bomb as provided in s. [790.165](#); 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 as provided in s. [790.166](#); 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 felony violation of s. [812.014](#); any violation of s. [790.07](#); 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 shall not be qualified for initial employment within or regular access to a seaport or restricted access area; and

2. 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 7 years prior to the employment or access date under consideration.

(d) 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, and any other material factors used in making the determination.

(4)(a) Subject to the provisions of subsection (6), each affected seaport shall begin to implement its security plan developed under this section by July 1, 2001.

(b) The Office of Drug Control and the Department of Law Enforcement may modify or waive any physical facility or other requirement contained in the statewide minimum standards for seaport security upon a finding or other determination that the purposes of the standards have been

reasonably met or exceeded by the seaport requesting the modification or waiver. Such modifications or waivers shall be noted in the annual report submitted by the Department of Law Enforcement pursuant to this subsection.

(c) Beginning with the 2001-2002 fiscal year, the Department of Law Enforcement, 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, and to identify seaport security changes or improvements necessary or otherwise recommended. The Department of Law Enforcement, or any entity designated by the department, may conduct additional announced or unannounced inspections or operations within or affecting any affected seaport to test compliance with, or the effectiveness of, security plans and operations at each seaport, to determine compliance with physical facility requirements and standards, or to assist the department in identifying changes or improvements necessary to bring a seaport into compliance with the statewide minimum security standards.

(d) By December 31, 2001, and annually thereafter, the Department of Law Enforcement, in consultation with the Office of Drug Control, shall complete a report indicating the observations and findings of all inspections or operations conducted during the year and any recommendations developed by reason of such inspections. A copy of the report shall be provided to the Governor, the President of the Senate, the Speaker of the House of Representatives, and the chief administrator of each seaport inspected. The report shall include responses from the chief administrator of any seaport indicating what actions, if any, have been taken or are planned to be taken in response to the recommendations, observations, and findings reported by the department.

(e) In making security project or other funding decisions applicable to each seaport listed in s. [311.09](#), the Legislature may consider as authoritative the annual report of the Department of Law Enforcement required by this section, especially regarding each seaport's degree of substantial compliance with the statewide minimum security standards established by this section. The Legislature shall review any seaport that is not in substantial compliance with the statewide minimum security standards by November 2005, as reported by the Department of Law Enforcement.

(f) By December 31, 2004, the Legislature shall review the ongoing costs of operational security on seaports, the impacts of this section on those costs, mitigating factors that may reduce costs without reducing security, and methods by which seaports may implement operational security using a combination of sworn law enforcement officers and private security services.

(g) Subject to the provisions of this chapter and appropriations made for seaport security, state funds may not be expended for operational security costs without certification of need for such expenditures by the Office of Ports Administrator within the Department of Law Enforcement.

(5) Nothing in this section shall be construed as preventing any seaport from implementing security measures that are more stringent, greater than, or supplemental to the statewide minimum standards established by this section except that, for purposes of employment and access, each seaport shall adhere to the requirements provided in paragraph (3)(c) and shall not exceed statewide minimum requirements.

(6) When funds are appropriated for seaport security, the Office of Drug Control and the Florida Seaport Transportation and Economic Development Council shall mutually determine the allocation of such funds for security project needs identified in the approved seaport security plans required

by this section. Any seaport that receives state funds for security projects must enter into a joint participation agreement with the appropriate state entity and must use the seaport security plan developed pursuant to this section as the basis for the agreement. If funds are made available over more than one fiscal year, such agreement must reflect the entire scope of the project approved in the security plan and, as practicable, allow for reimbursement for authorized projects over more than 1 year. The joint participation agreement may include specific timeframes for completion of a security project and the applicable funding reimbursement dates. The joint participation agreement may also require a contractual penalty, not to exceed \$1,000 per day, to be imposed for failure to meet project completion dates provided state funding is available. Any such penalty shall be deposited into the State Transportation Trust Fund to be used for seaport security operations and capital improvements.

History.--s. 1, ch. 2000-360; s. 1, ch. 2001-112; s. 1, ch. 2003-96; s. 1, ch. 2004-261.

Disclaimer: The information on this system is unverified. The journals or printed bills of the respective chambers should be consulted for official purposes. Copyright © 2000-2004 State of Florida.

TAB 6

**DISCUSSION OF FEDERAL FY 2005 PORT
SECURITY GRANT PROGRAM**



U.S. Department of Homeland Security Announces Over \$140 Million in Grants to Secure Ports

For Immediate Release
Office of the Press Secretary
Contact: Marc Short, 202-282-8010
May 13, 2005

The U.S. Department of Homeland Security today announced \$140,857,128 in port security grants. The FY 2005 Port Security Grant Program (PSGP) uses a risk-based formula to allocate funds to protect our ports from acts of terrorism. The program fortifies security at our nation's ports by providing funding to increase protection against potential threats from small craft, underwater attacks and vehicle borne improvised explosives, and to enhance explosive detection capabilities aboard vehicle ferries and associated facilities.

The new risk-based formula considers three elements: threat, vulnerability, and consequence. As part of this risk-management approach, the port security grant program will ensure federally regulated ports, terminals, and U.S. inspected passenger vessels receiving the funds represent assets of the highest national strategic importance. Sixty-six port areas have been identified as eligible applicants for inclusion in the FY 2005 program. Successful applicants will be awarded through a competitive process.

"Our nation's ports are centers for commerce, trade, and travel - areas our enemies could seek to attack in their attempts to defy freedom and liberty. These grants will help prepare and protect our nation to minimize risk and to win the war on terrorism," said Matt A. Mayer, Acting Executive Director of the Department of Homeland Security's Office of State and Local Government Coordination and Preparedness (SLGCP).

DHS designed this program in coordination with the Department of Transportation and the American Association of Port Authorities. DHS has collectively awarded \$489.4 million in previous rounds.

[\(Attachment A: Port Areas Eligible for Consideration of Funding\)](#)

###

Additional Guidance on Authorized Program Expenditures

This appendix serves as an additional guide for program expenditure activities. Grantees are encouraged to contact their ODP Program Manager regarding authorized and unauthorized expenditures.

A. Projects that Support the National Port Security Priorities

When developing project proposals for the FY 2005 PSG Program, specific attention must be paid to prevention and detection of attacks involving IEDs. IEDs pose a threat of great concern to transportation systems across the nation. IEDs have historically been the terrorist weapon of choice because they combine a high degree of effectiveness with minimal cost. Of greatest concern to port security are IEDs delivered via small craft, underwater and in vehicles on ferries. Particular areas of focus, therefore, should include protection of facilities, including public cruise line and ferry terminals, and vessels from tampering and attack.

The following are examples of security enhancements designed to enhance IED prevention and detection capabilities for port systems:

1. Port Facilities, Including Public Cruise Line and Ferry Terminals

- Explosive Agent Detection Sensors
- Chemical/Biological/Radiological Agent Detection Sensors
- Canines (start-up costs and training for terminal operations)
- Intrusion Detection
- Small boats for State and Local Law Enforcement Marine Patrol/Security Incident Response
- Video Surveillance Systems
- Security Entry/ID Systems
- Employee Identification
- Improved Lighting
- Secure Gates and Vehicle Barriers
- Floating Protective Barriers
- Underwater Intrusion Detection Systems (Excluding Sonar)
- Communications Equipment (including interoperable communications)

2. Vessels and Ferries

- Explosive Agent Detection Sensors
- Chemical/Biological/Radiological Agent Detection Sensors

- Restricted Area Protection (cipher locks, hardened doors, CCTV for bridges and engineering spaces)
- Communications Equipment (including interoperable communications)
- Canines (start-up costs and training for U.S. vehicle/passenger ferries)
- Floating Protective Barriers

B. Specific Guidance on Canines

Eligibility for funding of Canine Explosive Detection programs is restricted to U.S. Ferry's regulated under 33 CFR Parts 101, 104 & 105 specifically U.S. ferry vessels carrying more than 500 passengers with vehicles, U.S. ferry vessels carrying more than 2,000 passengers and the passenger terminals these specific ferries service. Additionally, only owners and operators of these specific ferries and terminals and port authorities or State local authorities that provide layered protection for these operations and are defined in the vessel's/terminal's security plans as doing so are eligible.

Certification: Canines used to detect explosives must be certified by an appropriate, qualified organization. Such canines should receive an initial basic training course and also weekly maintenance training sessions thereafter to maintain the certification. The basic training averages 10 weeks for the canine team (handler and canine together) with weekly training and daily exercising. Successful proposals must reflect that the canine explosive detection training program used is equivalent to or exceeds the training and certification standards recommended or in use by the state or local law enforcement agency in whose jurisdiction the screening will occur. Comparable training and certification standards, such as the National Police Canine Association (NPCA), the United States Police Canine Association (USPCA) or the International Explosive Detection Dog Association (IEDDA) may be used to meet this requirement.⁷

Agreement: Applicants are encouraged to thoroughly review the fiscal obligations of maintaining a long-term Canine Explosive Detection program. Successful applicants will be required to submit a signed Memorandum of Understanding to ODP acknowledging that PSG awards allow a one-time procurement to assist in implementing the Canine Explosive Detection teams. This one-time procurement authorization will be issued with the understanding that the applicant will maintain the canine's proficiency for explosives detection, and that any additional costs throughout the 8 to 10 year service life of the canine are the sole responsibility of the applicant.

Eligible Costs: Eligible costs include the purchasing, training and certification of canines; all medical costs associated with initial procurement of canines; kennel cages used for transportation of the canines and other incidentals associated with outfitting and set-up of canines (such as leashes, collars, initial health costs and shots etc.). Eligible costs also include initial training and certification of handlers.

⁷ Training and certification information can be found at: <http://www.npca.net>, <http://www.uspcak9.com/html/home.shtml>, and <http://www.bombdog.org/>.

Ineligible Costs: Ineligible costs include but are not limited to hiring, travel and lodging associated with training and certification; meals and incidentals associated with travel for initial certification; vehicles to transport canines; and maintenance / recurring expenses such as annual medical exams, canine food costs, etc.

C. Specific Guidance on Employee Identification

The Transportation Worker Identification Credential (TWIC) is designed to be an open architecture, standards-based system and follow published ANSI/NIST and ISO standards. Accordingly, port projects that involve new installations/upgrades to access control systems, should exhibit compliance to these and related standards in their system design and implementation. Port card reader systems should be compliant with ISO 7816 and/or ISO 14443 for appropriate TWIC smart card compatibility. The TWIC program will enable the use of biometric recognition technologies in port access control systems, following guidelines provided by the ANSI INCITS 383-2004 "Biometric Profile -Interoperability and Data Interchange -Biometrics based Verification and Identification of Transportation Workers" document. The TWIC program will be compliant to the GSC-IS (Government Smart Card Interoperability Standard), and associated efforts that include the GSC-IAB PACS (Interagency Advisory Board Physical Access Control Systems) implementation guidelines and ICC data model.

TAB 7

**REVIEW OF STATUS OF FLORIDA UNIFORM
PORT ACCESS/TWIC CARD**

The purpose of this document is to update each port with the details of the FUPAC implementation.

Legal Issues (housekeeping)

This implementation is a FUPAC implementation governed by Florida State Statute 311.125 which states:

1. “The Department of Highway Safety and Motor Vehicles, in consultation with: the Department of Law Enforcement the Florida Seaport Transportation and Economic Development Council the Florida Trucking Association, and the United States Transportation and Security Administration shall develop a Uniform Port Access Credential System for use in on-site verification of access authority for all persons on a seaport.”

As the law states, DHSMV has been mandated to develop and implement a system. DHSMV has been working on this for the past 22 months. Contrary to some opinions, this is certainly not a system being forced on anyone. DHSMV, acting as an advocate for the ports, has organized appropriate stakeholder committees, established managers with direct responsibility and even developed a website (WWW.Fupac.Info) with appropriate contact information for any port with a concern or question. DHSMV has even assisted ports by purchasing various systems and equipment. DHSMV is your advocate and is here solely to HELP YOU implement and be in compliance with the law.

2. “By July 1, 2004, each seaport shall be required to use a Uniform Port Access Credential Card.” and “Each seaport defined in s. 311.09 and required to meet the minimum security standards set forth in s. 311.12 shall comply with technology improvement requirements for the activation of the Uniform Port Access Credential System no later than July 1, 2004. Equipment and technology requirements for the system shall be specified by the department no later than July 1, 2003. The system shall be implemented at the earliest possible time that all seaports have active technology in place, but no later than July 1, 2004.”

Due to the unusual partnership formed with TSA, the final implementation date of this project has been delayed. DHSMV has provided numerous reports to Senate, House and oversight committees to keep everyone informed and to reassure the legislation and governor’s office that progress has been made. It is now time to deliver. TSA is ready, DHSMV is ready, FDLE is ready and the ports should be ready.

3. “Each seaport is responsible for the proper operation and maintenance of the Uniform Port Access Credential Card reader and access verification utilizing the Uniform Port Access Credential System at its location.”

Once implemented, each port needs to recognize the importance of maintaining their system. DHSMV recommends that the ports develop a separate administrative fee to

underwrite the cost of access control at each port. It should be noted that the maintenance of the GE Subhost as well as the readers provided by the state will be covered under a state contract.

4. “The price of a Uniform Port Access Credential Card shall be set by the department [DHSMV] and shall reflect the cost of the required criminal history checks, including the cost of the initial state and federal fingerprint check and the annual criminal history check and the cost of production and issuance of the card by the department. Seaports may charge an additional administrative fee to cover the costs of issuing credentials to its employees and persons doing business at the seaport.”

DHSMV will discuss the recommended fee structure further on in this document.

Florida/TSA arrangement

TSA has signed a unique partnership agreement with the state of Florida [DHSMV] which will provide equipment, software, services and credentials. Although this implementation is actually a FUPAC implementation it is also a TWIC prototype. Initially this will be a FUPAC card but will morph into a TWIC card in 12 to 18 months. Because of this unique arrangement, Florida and the ports will only have to implement the credential one time. Because of this the original credential period is 4 years but once TWIC takes authority, estimated to be 12 to 18 months, it will become a 5 year credential.

Infrastructure:

Once again, TSA has signed a unique partnership agreement with the state of Florida [DHSMV] which will provide equipment, software, services and credentials. In return Florida will assist TSA in their prototype by allowing special readers to be placed in specific locations in each port. These readers **MUST** have the capability to collect metrics which will allow TSA to gather information. This information will assist TSA in moving forward with appropriate recommendations. Each port must do everything possible to meet the infrastructure requirements necessary for TSA. DHSMV has highlighted this requirement for over one year. Infrastructure has been a major requirement since it was raised at our port implementation committee meetings last March, it was a major element of our meeting in Boca Raton in August and has been on the front page of our website since September 2004. We must do everything possible to assist TSA in collecting their metrics prior to June 30, 2005, the deadline for their Prototype.

Credentials:

DHSMV has collected badging files from all ports up to October 2004. DHSMV also collected Fingerprint files from FDLE. These files were merged and over 14,000 credential records were provided to TSA for automated enrollment. We call these records the “Legacy” records. TSA began enrolling legacy personnel on March 28th, 2005.

These credentials will begin to arrive at your port shortly. You must:

1. **Immediately designate a person responsible to receive these credentials.** This should be provided today to Billy Dickson and the TSA representative, Ed Cook.

2. Lock these credentials in the enrollment center safe until TSA Trusted Agents can come to your port and active these credentials.
3. Credential activation units will be installed in the ports over the next few weeks.
4. When ready to activate **you need to notify these personnel to come in to get their credentials**. Therefore, while you are waiting for activation personnel you should consolidate the list of credentials and develop an approach to notify these personnel to come in and pick up their credentials.
5. You need to provide the badging information once again to bring the files up to date and automatically convert as many as possible. Please send these files to Scott Bean at DHSMV (850) 414-8046. Scott will attempt to match these to newly acquired FDLE files and once again automatically convert as many as possible. If you have trouble pulling your files then contact Scott and he will make arrangements for you.
6. These automatically converted credentials will have an expiration date within the next year. This date will coincide with their existing expiration date. DHSMV and TSA will not charge for these credentials. The cardholder has paid for permission up to a specified expiration date so these cards will be free of charge up to that date.
7. Upon their expiration date they will be required to come into the enrollment center and be reissued a new four year credential. At that time they will pay the estimated fee of \$85 for a 4 year credential. This will cover the background check and associated cost of creating and maintaining the credential.
8. There will be a recurring \$6 name based background check each year thereafter. FDLE has created an automatic system for notification of violations and billing. You will be contacting you shortly to work out the final details.

Unfortunately due to incomplete records, quality of prints or potential for adjudication, certain existing cardholders could not be automatically converted. Estimates range from 50% to 80% conversion capability. This means that some portion of your credential population will need to come into the enrollment center and enroll for a 4 year card immediately. We, and you, can identify the full enrollment personnel as soon as we finalize creating all the legacy credentials (automatically converted personnel).

Trusted Agents & Adjudicators:

You need to identify immediately your Trusted Agents and Adjudicator. DHSMV realizes that you have already provided the names of several personnel. We are asking you to review these names to ensure they are the personnel who will actually be enrolling candidates. Col. Dickson will finalize these names today and schedule training.

Picture Perfect System

All ports have a GE Picture Perfect system installed. DHSMV is currently making arrangement for training on this new system. We are trying to make sure training is as close as possible to your ports implementation date. Three ports have already been trained. Al Brignoni will be contacting all ports to schedule training.

Once your personnel are trained you will be visited by a representative of DHSMV, either a consultant or a technician, who will assist you in creating your access schema in accordance with

the state color codes (derived from the FSTED recommendations). They will also assist you in establishing your own port specific access schema.

Note: GE has released an update to this system which is Version 3.0. It is more user friendly and has several additional upgrades and capabilities. DHSMV is evaluating the upgrade of this system but will not undertake the upgrade until the implementation is complete.

Standard Operating Procedures

TSA has taken the Florida SOPs and built the TSA TWIC SOPs. These SOP documents do not dictate anything; they are a guideline to assist in utilizing the equipment and procedures. They will be provided to all Trusted Agents at the ports. As you utilize and review these documents please forward any recommendations or changes to Jim Kneeland at DHSMV

Readers

TSA is prepared to install readers in all TSA indicated locations. These locations must have an infrastructure in place which supports activating gates and collecting metrics (cat 5 requirements). If you need WIU boards or panels then please notify Al Brignoni at (850) 591-5627.

The Florida Reader Competitive Procurement

DHSMV has constructed an ITB which was released on Friday 4/8/05. The award will be made in May 2005 and DHSMV will immediately begin to distribute new biometric readers. We have approximately \$500K for readers in FY 2005 and \$1.2 million for the following year(s). The ITB is built to acquire both fixed and wireless/handheld readers. We anticipate providing readers over the next 2 years as infrastructure continues to be built out. A committee will be formed for distribution of the readers to the needed locations at each port. We will ask FSTED to coordinate this.

FUPAC/TWIC PROTOTYPE IMPLEMENTATION

Fees:

The following illustrates the recommended fee structure:

Entity	Reason	Cost
FDLE	Background Checks	\$47
HSMV	Annual Recurring Expenses (Maintenance, T1s etc)	\$28
Ports	Underwrite Enrollment Personnel	\$10
Estimated Total Credential Cost:		\$85 for a 4 year credential

Note: The \$10 port fee is to underwrite the expense of the person manning the enrollment center and collecting the credential information. This fee DOES NOT underwrite the expense of the access control system and should be a separate fee set by the port which will cover the expenses of maintaining the access control infrastructure. Some ports are handling the access control system expenses through a tariff.

The overall fee is subject to change when TSA mandates the TWIC

Implementation Steps

The following illustrates the actual implementation steps we anticipate over the next 4 to 6 weeks:

1. Produce Legacy Cards – These are currently being created by TSA
2. Collect remaining legacy files – so we can automatically convert as many as possible
3. Train TSA Trusted Agents – so they can activate first batch of legacy cards
4. Send Activation Units to Ports – These are the units that allow fingerprint verification at card activation time and is in process
5. Activate Legacy Credentials – TSA Trusted agents will start as soon as they finish training
6. Train Florida TAs – now that the TSA TAs are trained we will start training Fl personnel in May
7. Train Florida Personnel on Picture Perfect – Already started. 3 ports are trained already. Al Brignoni will contact you to set up your training (if needed)
8. Finalize User Acceptance Test – in process
9. Set up Port Permission Schema
10. Activate or Flash Readers
11. Finalize Fee Issues – a communiqué will be released within one week.
12. Switch Crossmatch Readers to TSA Enrollment Centers
13. Enroll Personnel with a four year credential

**When in doubt about
anything
call your DHSMV
manager**



Implementation Information

There appears to be some confusion about TWIC and FUPAC. The following will hopefully clear up any confusion:

FUPAC (Florida Uniform Port Access Credential) is mandated by Florida Statute 311.125 which mandates that ports **MUST be in compliance with a statewide biometric credential by July 1, 2004.**

TSA is currently implementing the FUPAC which will become a TWIC card once TSA rulemaking is complete. It is no mistake that the credential being issued says TWIC. TSA is working as a partner with Florida to issue the FUPAC as a TWIC card under F.S. 311.125.

In other words, TWIC = FUPAC and FUPAC = TWIC

If you have any questions contact your Florida project manager listed below:

IMPLEMENTATION TEAMS:

There are three (3) primary installation teams. They are:

- **Team 1 Team Leader is Jim Kneeland (850) 591-9594 and ports in Team 1 are:**
 - Port of Pensacola**
 - Port of Panama City**
 - Port of Jacksonville**

Port of Fernandina

- **Team 2 Team Leader is Billy Dickson (850) 251-5682 and ports in Team 2 are:**
- **Port of Canaveral**
- **Port of Tampa**
- **Port Manatee**
- **Port St Pete**
- **Team 3 Team Leader is Al Brignoni (850) 591-5627 and ports in Team 3 are:**
- **Port of Palm Beach**
- **Port Everglades**
- **Port of Key West**

TAB 8

**DISCUSSION OF CARIBBEAN BASIN MARITIME
SECURITY ISSUES**

 **Florida Ports**
C O U N C I L
502 East Jefferson Street, Tallahassee, Florida 32301
Telephone: (850) 222-8028
Fax: (850) 222-7552
www.flaports.org - E-Mail: info@flaports.org

MEMORANDUM

DATE: June 1, 2005
TO: Florida Port Directors
FROM: John R. LaCapra
SUBJECT: **EQUIPMENT CONTRIBUTIONS/HAITI MARITIME SECURITY**

The USAID funded maritime security program in Haiti has requested equipment contribution to the Haitian government which would provide maritime security assistance.

We list below the types of equipment which have been suggested to assist the Haitian government.

List of Equipment

- 1) Generators - Diesel 250kw.
- 2) Patrol Boats - 20 or 30 feet long.
- 3) Radio Communication Equipment - Handheld VHF, SSB (Single Side Band) with Repeater, and Radio Bases.
- 4) Security Wands.

We request that each Florida port might review its surplus equipment and appropriate surplus equipment procedures in order to evaluate whether any of the above equipment needs may be contributed to Haiti.

Your assistance will benefit the efforts of the Caribbean Central American Action (CCAA) and Florida Ports Council (FPC) to assist in the development of maritime security in Haiti.

Thank you.

JRL/rds

N:\FPC Meetings\FPC Meeting - Fernandina - 6-8-05\Haiti Equipment Memo.wpd

TAB 9

OTHER ISSUES

Subj: **Seaport Security Training at Port Manatee Now MARAD Certified**
 Date: 6/2/2005 4:25:18 PM Eastern Daylight Time
 From: CHRISSEY@Portmanatee.com
 To: njl50@aol.com
 File: **SecuritytrainingMARADcertification-letterheadFINAL.doc** (305152 bytes) DL Time (TCP/IP): < 1 minute
Sent from the Internet ([Details](#))

June 1, 2005

MORE INFORMATION CONTACT:

Chrissy Kruger-Gruendyke, APR, Communications Specialist
 Port Manatee
 (941) 722-6621 / (941) 650-7306

PORT MANATEE IS NATION'S FIRST SEAPORT TO EARN MARAD SECURITY TRAINING CERTIFICATION

PALMETTO, Fla. – Port Manatee today became the nation's first seaport receiving certification from the U.S. Maritime Administration (MARAD) for its seaport security training coursework.

The port's training courses comply with the congressional Maritime Transportation Security Act of 2002 (MTSA) and International Ship and Port Facility Security (ISPS) code. Training is based on curriculum models provided by MARAD.

"This is a significant achievement for Port Manatee and the U.S. seaport community," said Executive Director David L. McDonald PPM®. "We have one of the most qualified security teams in the nation, which is being looked upon to train seaport security personnel from across the U.S."

Port Manatee submitted the demanding 750-page certification application in April 2005. All aspects of the course's planning and implementation including course materials, instructor qualifications and classroom facilities were evaluated.

"Port Manatee has shown true leadership and vision in receiving this important certification," said U.S. Congresswoman Katherine Harris, a member of the House Committee on Homeland Security. "They have worked immensely hard to distinguish the port as a leader in Homeland Security and I will continue to work hard to ensure that they remain a leader in port security by ensuring they have the adequate funding needed to carry out their goals."

The comprehensive training program is already attracting professionals from ports throughout the U.S.

"Educating and updating port employees on maritime security is critical for the health of the maritime community, and for winning the war on terrorism," said MARAD Acting Administrator John Jamian. "We encourage other facilities to follow the example set by Port Manatee."

"The certification ensures that security personnel who complete our courses meet all federal training requirements," said the port's Director of Seaport Security, Frank Holden. "These efforts lay the groundwork for Port Manatee to expand its training programs and work toward creating a maritime security academy."

The security training initiative is just one example of Port Manatee's cutting-edge approach to security since 2002. The port also enhanced its staff, security plan and access control systems while serving as a research and development site for new security technology.

The improvements are garnering attention not only from MARAD, but also the U.S. Coast Guard, Florida Department of Law Enforcement and the American Association of Port Authorities.

"We congratulate Port Manatee, which is a long-time member of AAPA, for being the first seaport in the country to receive the U.S. Maritime Administration's certification to provide this level of federally-compliant security training," said AAPA President and CEO Kurt Nagle.

Notes: The security training curriculum and materials are confidential as part of the port's security plan and therefore exempt from public records laws. A general description of the course is available at www.portmanatee.com.

The media may contact the following for additional comment: for **U.S. Congresswoman Katherine Harris**, contact Garrison Courtney, 202-374-1454; for **MARAD Acting Administrator John Jamian**, contact Susan Clark at 202-366-5807; for **AAPA President and CEO Kurt Nagle**, contact Aaron Ellis, 703-706-4714.

###

Chrissy Kruger-Gruendyke, APR
Communications Specialist
Port Manatee
300 Tampa Bay Way
Palmetto, Florida 34221
Office: (941) 722-6621 ext. 319
Cell: (941) 650-7306
Fax: (941) 729-1463
chrissy@portmanatee.com
<http://www.portmanatee.com>

TAB 10

ADJOURNMENT