HB 1683 2004 A bill to be entitled

1

2

3

4 5

6

7

8

9

10

11

12 13

14

15

16 17

18

19

20

21

22

23

An act relating to seaport security standards; amending s. 311.12, F.S.; requiring that each seaport security plan

have a procedure that notifies an individual that he or she is disqualified from employment within, or regular

access to, a seaport or a seaport's restricted access

area; requiring each plan to include a procedure by which

the individual may appeal the decision of the seaport;

directing a seaport to have its procedures in substantial

compliance with federal regulations; providing criteria

for seaports to consider for inclusion in procedures for

appeals and waivers from disqualification; providing that

an individual remain free from subsequent convictions for

5 years before seeking employment in, or access to, a

seaport; requiring each seaport to report to the

Department of Law Enforcement by a specified date the

number of waivers from disqualification issued in the

previous 12 months; amending s. 311.125, F.S.; conforming

provisions to changes made by the act; reenacting s.

315.02(6), F.S., relating to the definitions for the 1959

Port Facilities Financing Law, for the purpose of

incorporating the amendment to s. 311.12, F.S., in a

reference thereto; providing an effective date.

24 25

Be It Enacted by the Legislature of the State of Florida:

26

27

Section 1. Section 311.12, Florida Statutes, is amended to read:

28 29

Seaport security standards. --

Page 1 of 19

 (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, under 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 under pursuant to subsection (1). Each plan adopted or revised under 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 these 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 under 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, the 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

88

89

90

91 92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

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 (e) (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. These 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) Each seaport security plan shall establish a procedure that notifies an individual that he or she is disqualified for employment within or regular access to a seaport or restricted

HB 1683

access area. The plan shall also include a procedure by which
the individual may appeal the decision of the seaport. The
procedures must be in substantial compliance with 49 C.F.R.,
Part 1572, and must include, but need not be limited to, the

following:

procedures.

- 1. The seaport must notify the individual, in writing,
 that he or she poses a security threat to the seaport and is
 disqualified for employment in or access to the seaport. The
 notification must include a statement that the seaport has
 determined that the individual poses a security threat
 warranting disqualification, the basis for the determination,
 and information about the correction of records and appeal
 - 2. An individual may appeal a disqualification determination only if the individual asserts that he or she meets the qualifications set by the seaport for the position for which he or she is applying. If the disqualification determination is based on a conviction for a disqualifying crime listed in paragraph (e), the individual may present evidence that the underlying criminal record is incorrect, or that the conviction was pardoned, expunged, or overturned on appeal. An executive pardon, expungement, or overturned conviction may nullify a disqualifying conviction if the pardon, expungement, or overturned convictions on the individual.
 - 3. An individual may initiate an appeal of a disqualification determination by submitting a written request for materials or a written reply to the seaport within 15 days after receiving notification of the disqualification

determination. If the individual does not initiate an appeal within that time, the decision of the seaport is final.

- 4. The individual may serve upon the seaport a written request for copies of the materials upon which the disqualification determination was based. If the disqualification determination was based on a state or Federal Bureau of Investigation criminal history record that the individual believes is erroneous, the individual may correct the record and submit the corrections to the seaport. The seaport must respond within 30 days after receiving the individual's request for materials. The seaport must give the individual a copy of the releasable materials upon which the disqualification determination was based. The seaport may not include any classified information as provided by federal law.
- 5. The individual may also serve on the seaport a written reply to the disqualification determination stating that the seaport made errors when it issued the disqualification determination.
- 6. The seaport must respond to the individual's appeal no later than 30 days after the seaport receives an individual's request. If the seaport determines that the individual does pose a security threat, the seaport shall give written notice to the individual of its final decision that the individual is disqualified for employment in or access to the seaport. If, upon reconsideration, the seaport concludes that the individual does not pose a security threat to the seaport, the seaport must notify the individual in writing of its decision. Thereafter, the seaport shall issue to the individual the appropriate Uniform Port Access Credential Card.

7. If the seaport determines that the individual does pose a security threat, the seaport must include in its written notice of disqualification that the seaport's decision is final agency action subject to judicial review under s. 120.68.

- (d) 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 paragraph must be included in the seaport security plan. The seaport must consider, when determining whether to grant a waiver, if the disqualification is based on a disqualifying criminal offense, the circumstances of the disqualifying act or offense, whether restitution was made by the individual, and other factors that indicate that the individual does not otherwise pose a security threat warranting disqualification for access to the seaport. The seaport must send a written notice to the individual informing the individual whether the seaport granted or denied the request for a waiver. All waivers granted under this paragraph must be reported to the Department of Law Enforcement within 30 days after issuance.
- $\underline{\text{(e)}(\text{e})}$ In addition to other requirements for employment or access established by each seaport $\underline{\text{under}}$ $\underline{\text{pursuant to}}$ 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 <u>is shall</u> 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 is 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 5 at least 7 years before prior to the employment or access date under consideration.
- <u>(f)(d)</u> 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 <u>and any determination to issue a waiver</u> 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.

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

- 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. The Such modifications or waivers shall be noted in the annual report submitted by the Department of Law Enforcement under 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 under 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 these 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.
- (5) Nothing in This section does not prevent 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)(e) (3)(c) and may shall not exceed statewide minimum requirements.
- (6) When funds are appropriated for seaport security, the Office of Drug Control and the Florida Seaport Transportation

289

290

291

292

293

294

295

296

297

298

299300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316 317

and Economic Development Council shall mutually determine the allocation of these 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 under pursuant to this section as the basis for the agreement. If funds are made available over more than one fiscal year, the 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.

Section 2. Section 311.125, Florida Statutes, is amended to read:

311.125 Uniform Port Access Credential System. --

(1) By July 1, 2004, each seaport identified in s. 311.09 and subject to the statewide minimum seaport security standards set forth in s. 311.12 shall be required to use a Uniform Port Access Credential Card that is to be used utilized in the operation of the state Uniform Port Access Credential System as required herein. All Uniform Port Access Credential Cards shall

be issued by the Department of Highway Safety and Motor Vehicles to the designated port authority, or recognized governing board, of the requesting seaport for distribution to the credential applicant.

322

323

324

325

326

327

328329

330

331

332

333

334

335

336

337

338

339

340

341

342

343344

345346

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 Security Administration shall develop a Uniform Port Access Credential System for use in onsite verification of access authority for all persons on a seaport as defined in s. 311.12(2), using utilizing the Uniform Port Access Credential Card as authorized herein. Each seaport, in a manner consistent with 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, under pursuant to s. 311.12, and this section, is responsible for granting, restricting, or modifying access authority provided to each Uniform Port Access Credential Card holder and promptly communicating the levels of access or changes in the level of access to the department for its use in administering the Uniform Port Access Credential System. 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. The Uniform Port Access Credential Card reader and Uniform Port Access Credential System shall be used utilized by each seaport to ensure compliance with the access restrictions provided by s. 311.12.

(b) The system shall be designed to conform, as closely as possible, with criteria established by the United States
Transportation Security Administration for a Transportation
Worker Identification Card, or similar identification, as required by federal law. The system shall, at a minimum, consist of:

- 1. A centralized, secure database for collecting and maintaining fingerprints and other biometric means of identity, and other information pertaining to personal identification of persons working on, or doing business at, a Florida seaport as set forth in s. 311.12;
- 2. A methodology for receiving data from each port and transmitting data to each port regarding access permissions;
- 3. Technology required for each gate and portal at each seaport to be interactive with the Uniform Port Access Credential System during all hours of operation;
- 4. The ability to identify persons who have violated the access requirements of s. 311.12 and to deactivate the access permissions of those persons; and
- 5. The ability to $\underline{\text{use}}$ $\underline{\text{utilize}}$ the Uniform Port Access Credential Card in a manner consistent herein.

<u>The Such</u> system shall be designed to ensure the credentialed cardholders' privacy in a manner consistent with the state's security requirements as provided herein.

(3) The Uniform Port Access Credential Card must include at a minimum a digital fullface photograph, a digital fingerprint, a multilayered security process, a two-dimensional barcode with technology specifications that will allow the

unique biometric identifiers to reside in the barcode, a unique identifying code or number, scanning capability to compare required identifiers with information on file in the central database, and background color differentials for visual identification of access permissions.

- (4) A fingerprint-based criminal history check shall be performed on an applicant for a Uniform Port Access Credential Card as provided in s. 311.12(3). Based upon review of the criminal history check, each seaport may determine the specific access permissions that will be granted to that applicant. Upon receipt of a port authority "Notification of Access Permission" form and a verification of the criminal history check, the department shall issue a Uniform Port Access Credential Card to the port authority for distribution to the applicant.
- years following the date of issuance. Criminal history checks may be performed on a random basis, but at least once a year, during the period that the such credential card is active to ensure that the credential holder complies with the requirements for access to restricted areas provided in s. 311.12(3). Failure to complete any part of the required credential application process, or failure to comply with the criminal history clearances, shall be grounds for immediate denial of access. In addition to access authority granted to seaports, access authority may be restricted or revoked by the Department of Highway Safety and Motor Vehicles or the Department of Law Enforcement if the cardholder is suspected of criminal violations that could affect the security of a port or that otherwise render the cardholder ineligible for port access, upon

405

406

407

408

409

410

411

412

413414

415416

417

418

419

420

421

422

423

424

425

426

427

428429

430

431

432

thereof.

suspicion that the person in possession of the card is using it, or attempting to use it, fraudulently, or if restriction or revocation is done to assure the security of any port or portion

- Corporations, persons, or other business entities that employ persons to work on, or do business at, seaports regulated in s. 311.12 shall notify those seaports for which those employees have access permissions in the event of the employee's termination, resignation, work-related incapacitation, or death. Uniform Port Access Credential Card accesses for persons not currently employed to perform a job on a seaport shall be placed in an inactive status. Upon notification of a work status change, the port authority, or recognized governing board, shall notify the department to have the credential card placed in an inactive status. Inactive status shall continue until the expiration of the credential card or reactivation of the card by petition. The former employee may have the credential card reactivated by petitioning a seaport. The port authority, or recognized governing board, of any seaport may determine that the individual is employed by another appropriate entity or is self-employed for purposes of performing work on the seaport. Upon that determination, the port authority, or recognized governing board, may request reactivation of credentialing permissions. All these such cards may be restricted or revoked as provided in subsection(5).
- (7) Failure to report a change in work status, as defined in this section, within 7 days after the action may result in revocation of the business entity's access to the seaport.

433

434

435

436

437

438

439

440

441

442

443444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

Each person working on a seaport, as regulated in s. 311.12(2), shall be issued a Uniform Port Access Credential Card upon completion of the application process. Upon issuance of the Uniform Port Access Credential Card, the cardholder is eligible to enter a seaport in the system based on the level of permission allowed by each respective seaport. A person working in a restricted access area must meet the requirements of s. 311.12(3). The Uniform Port Access Credential Card shall be clearly marked for visual verification of the cardholder's permission for access to a restricted area, under pursuant to subsection (3). The card must contain biometric verification of the cardholder's identity and proper access permissions. Entrance to a restricted access area, as defined in s. 311.12(2), shall require a machine check and fingerprint verification of each person's Uniform Port Access Credential Card for proper identification. Exit from any restricted access area of a seaport shall require a machine check of the credential card.

(9) Each person not producing a Uniform Port Access
Credential Card upon arrival at a restricted area of a seaport
must, at a minimum, stop at a check point, show valid
identification, and receive a visitor's pass in order to
proceed. The visitor's pass must be plainly displayed on the
person of the visitor or in the windshield of the vehicle and
designate what area of the seaport may be accessed by the
visitor. Failure to display the visitor's pass shall result in
revocation of a worker's permission to work on the seaport.
Public conveyances such as buses carrying passengers into
restricted access areas must be able to verify that all

passengers have legitimate business on the seaport. Procedures for implementation of this process are the responsibility of each seaport.

- shall be set by the department 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. A seaport may charge an additional administrative fee to cover the costs of issuing credentials to its employees and persons doing business at the seaport.
- (11) Each Uniform Port Access Credential Card remains the property of the State of Florida. Any person possessing such a card shall provide it to any law enforcement officer upon request. A law enforcement officer having reasonable suspicion to believe that a card is possessed or is being used in violation of law or the standards provided by this section, or in any other manner that raises a concern about the safety and security of a seaport, may seize the card. A cardholder has no cause of action against any law enforcement officer who seizes a Uniform Port Access Credential Card.
- (12) 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.

- (13) 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, under pursuant to s. 311.12, shall be updated by the Department of Law Enforcement to reflect the changes made by this act.
- (14) This section shall be contingent on the receipt of the federal grant funds necessary to implement the Uniform Port Access Credential System.
- Section 3. For the purpose of incorporating the amendment to section 311.12, Florida Statutes, in a reference thereto, subsection (6) of section 315.02, Florida Statutes, is reenacted to read:
- 315.02 Definitions.--As used in this law, the following words and terms shall have the following meanings:
- (6) The term "port facilities" shall mean and shall include harbor, shipping, and port facilities, and improvements of every kind, nature, and description, including, but without limitation, channels, turning basins, jetties, breakwaters, public landings, wharves, docks, markets, parks, recreational facilities, structures, buildings, piers, storage facilities, including facilities that may be used for warehouse, storage, and distribution of cargo transported or to be transported through an airport or port facility, security measures identified pursuant to s. 311.12, public buildings and plazas, anchorages, utilities, bridges, tunnels, roads, causeways, and any and all property and facilities necessary or useful in connection with the foregoing, and any one or more or any

HB 1683 2004 combination thereof and any extension, addition, betterment, or 520 improvement of any thereof. 521 522 Section 4. This act shall take effect July 1, 2004.

Page 19 of 19

CODING: Words stricken are deletions; words underlined are additions.