The Florida Senate

Interim Project Report 2007-111 *October 2006*

Committee on Military Affairs and Domestic Security

INTERMODAL, POINT TO POINT, CARGO SECURITY

SUMMARY

International and domestic movement of cargo relies on the quick and efficient use of containerization. Cargo containers travel using a variety of shipping modes including vessels, truck, and rail.

Cargo containers at intermodal transfer points present opportunities for security breaches and a potential for smuggling of contraband and weapons of mass destruction. A layered international security system strategy has been developed to respond to this threat.

In the U. S., participants in the layered supply chain security system include federal, state, and local government executive agencies and law enforcement, port operators, private sector manufacturers and shippers, and the transportation industry including truck, rail, and vessel.

The goal of this layered security system is to extend the security perimeter as far off-shore from U. S. ports as possible. To accomplish this, a number of security strategies and programs have been established by the federal government. State and local entities and the private sector also have important security roles to play as containers move from U. S. ports, through the highway and rail systems, to their final destinations.

Cargo container security has improved since September 11, 2001. However, vulnerability remains in the system, requiring attention and improvement.

BACKGROUND

There is growing concern that the federal government's response to point of entry cargo security has not been adequate for the threat posed by the shipment of goods, weapons, or humans into our country. The threat is intermodal, including ships, ports, truck, trains and air cargo transport, as containers and palletized cargo can be moved easily among these different types of transportation.

Intermodal Systems Transfer Containers from Ships to Trucks or Trains

According to the Florida Department of Transportation, "Intermodal transportation is the use of more than one mode of transportation with a transfer(s) between modes to make a trip or complete a freight movement. For intermodal transportation to be effective, the transfer has to be convenient and efficient."[1]

Cargo containers provide that convenient and efficient means of delivering goods. They are essential to today's "just-in-time" supply chain, moving almost 90 percent of the world's manufactured goods.[2]

Cargo container security begins at the manufacturer's production facility and ends with delivery at the final destination. Cargo moving throughout the supply chain is always subject to theft, vandalism, or tampering.

Currently, there is much focus on cargo security at domestic seaports because the ports are constriction points and represent targets on U. S. soil. In fact, the Government Accountability Office (GAO) summarized this concern in testimony before Congress.

"Many seaport areas are inherently vulnerable, given their size, easy accessibility by water and land, large numbers of potential targets, and proximity to urban areas. Also, the large cargo volumes passing through seaports, such as containers destined for further shipment by other modes of transportation such as rail or truck, also represent a potential conduit for terrorists

[1] Florida Department of Transportation, *Year 2020 Florida Statewide Intermodal System Plan Interim Final Report*, March 1, 2000, page 2.
[2] U.S. Customs and Border Protection, *Fact Sheet*, March 29, 2006. www.cbp.gov

to smuggle weapons of mass destruction or other dangerous materials into the United States. The potential consequences of the risks created by these vulnerabilities are significant as the nation's economy relies on an expeditious flow of goods through seaports. A successful attack on a seaport could result in a dramatic slowdown in the supply system, with consequences in the billions of dollars."[3]

However, it is important to note that freight, particularly in cargo containers, travels by truck and rail as well as by ship. Thus cargo security efforts apply to all aspects of intrastate, interstate, and international commerce.

This report, therefore, reviews federal and state cargo inspection activities in order to determine if more state or local action is required.

METHODOLOGY

Interviews were conducted with Department of Transportation Motor Carrier Compliance and Rail Office staff and Department of Agriculture and Consumer Services Law Enforcement staff. Site visits were conducted to observe FDOT and DOACS regulatory and inspection operations at agency locations along Interstate 10. Interviews were conducted with rail and trucking industry representatives including CSX Corporation and Landstar System Inc. Site visits and interviews were conducted at the following Florida ports: Port of Jacksonville, Port of Tampa, Port of Miami, Port Everglades, Port of Palm Beach, and Port Canaveral. Interviews at these ports included port management and security personnel, local law enforcement personnel, U. S. Customs and Border Protection and U. S. Coast Guard personnel, and resident FDLE agents. Each port visit included a port tour and observation of security infrastructure and procedures. Committee staff attended the 5th North American Cargo Security Forum. Presentations included current private sector cargo security issues and concerns, federal government cargo security and anti-terrorism initiatives and programs, emerging container security technologies, and discussions with industry representatives. Committee staff interviewed a member of the Miami-Dade Police Department Cargo Theft Task Force. Committee staff also performed an extensive literature search for this project.

FINDINGS

Security Can Easily be Compromised in Containers Primarily Designed for Speed and Efficiency

An axiom of the shipping industry is "A box at rest is a box at risk."

Steel constructed dry shipping containers may or may not have locks to secure their doors. Usually they do not have locks. Industry practices, however, require some form of serialized seal device that once installed must be cut to allow door opening. Seals are not meant to serve as locks. They simply provide accountability of door opening.

There are innumerable ways to tamper with seals and containers. A counterfeit replacement seal can have its serial number shaved off and re-stamped with the original seal's number. A bolt seal can have its locking pin removed and resealed with epoxy glue to give the appearance of seal integrity. A thin metal foil seal can be treated with salt water to render its serial number unreadable.

Containers can be tipped on their sides and entered through the bottom by cutting into them. Door hasp bolts can be drilled out and replaced. A simple home made tool can be used to pry open the right side door tab that blocks the left side door from opening. Once accomplished, the left side door can be opened and closed without disturbing the right side door seal.

Containers by themselves are not secure. Container security is achieved by developing a layered system.

Layered Container Security Requires Government and Industry Collaboration

The layered container security system currently in place in the U. S. requires a cooperative partnership between federal, state, and local government entities, the private sector and ports in other countries. Each partner has a defined role and provides certain resources and capabilities needed to build a layered security system.

The Federal Government's Role

The federal government's responsibility for intermodal container security and anti-terrorism activity begins at

[3] GAO, *Maritime Security: Enhancements Made, But Implementation and Sustainability Remain Key Challenges*, GAO-05-448T, (Washington, D.C., May 17, 2005).

the foreign manufacturer's production facility. It continues through foreign ports and U. S. ports of entry and ends at final delivery after the cargo travels through interstate commerce via truck, rail, or vessel.

The current federal government goal is to expand the security perimeter as far as possible offshore. General policy reflects that once a suspicious container reaches a U. S. port, it may be too late to prevent an attack. Federal government tasks, necessary to fulfill its role, therefore include development and dissemination of intelligence, cargo screening and inspection, and cargo entry clearance.

The Department of Homeland Security Attempts to Move the Security Perimeter Offshore

The federal government began to introduce programs to improve national security immediately after the events of September 11, 2001. This resulted in a major governmental reorganization that established the Department of Homeland Security (DHS). Many functions associated with national security were transferred to DHS including customs, coast guard, immigration, and emergency preparedness. The customs function was reconstituted within DHS as the U. S. Customs and Border Protection (CBP). CBP now has overall responsibility for establishing cargo container security programs.

CBP has employed multiple strategies in an attempt to prevent the importation of weapons of mass destruction (WMD). As the GAO stated, "there is heightened concern that terrorists will attempt to smuggle a weapon of mass destruction (e.g., a nuclear, biological, or radiological explosive device) into the United States using one of the 11 million cargo containers that arrive at our nation's seaports. Because of the large volume of imported containers, CBP maintains that it is unable to physically inspect all oceangoing containers without disrupting the flow of commerce."[4] CBP's current capabilities are reflected in the following programs.

The agency has developed and continues to improve its Automated Targeting System (ATS) for administrative screening of cargo containers. Associated with ATS is the "24 Hour" rule and a program called the Compliance Management Program. Two other CBP programs known as the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) complete the attempt to layer a defense and move WMD identification and interdiction offshore.

ATS Functions as a Screening Decision Tool

The Automated Targeting System is a complex computer model used by CBP to review information, including electronic manifest information, submitted by the ocean carriers on all arriving shipments. This information is used to help identify containers for additional inspection. CBP requires the carriers to submit manifest information 24 hours prior to loading a United States-bound sea container onto a vessel in a foreign port.[5]

CBP officials reported to committee staff that their goal is to screen 100% of all cargo containers entering the United States. From this screen, high risk containers are targeted to receive further non-intrusive inspection using gamma-ray or x-ray scanning technology or physical inspection.

The "24 Hour" rule for receipt of cargo manifest information now allows CBP to conduct an ATS screen to identify high risk containers. The Compliance Measurement Program introduces a random selection component to the screening process. Additional containers are randomly selected for physical screening beyond those already judged high risk.[6]

The Container Security Initiative Stations CBP Officers in Foreign Ports

The Container Security Initiative (CSI) deploys teams of CBP officers overseas to work with host nation counterparts in targeting containers that pose a potential threat.[7] The four core elements of CSI are:

- Identify high-risk containers using ATS.
- Prescreen and evaluate containers before they are shipped.
- Use large scale gamma-ray, x-ray, and radiation detection devices to rapidly scan high-risk containers without slowing down the movement of trade.

[4] GAO, *Cargo Container Inspections: Preliminary Observations of the Status of Efforts to Improve the Automated Targeting System*, GAO-06-591T, (Washington, D.C., March 30, 2006).

[5] Ibid., page 5.
[6] Ibid., page 1.
[7] U.S. Customs and Border Protection, *Fact Sheet*, March 29, 2006. www.cbp.gov

- Use smarter, more secure containers, to allow CBP officers to better detect containers that have been tampered with during transit.

As of March 29, 2006, CBP had 44 foreign ports participating in the program with a goal of 50 ports by the end of 2006. To be eligible to participate, a candidate nation must:

- Be able to inspect cargo using non-intrusive inspection equipment and radiation detection equipment.
- Have regular, direct, and substantial container traffic to ports in the U. S.
- Commit to establishing a risk management system to identify potentially high-risk containers.
- Commit to sharing critical data, intelligence, and risk management information.
- Conduct a thorough port vulnerability assessment and resolve those vulnerabilities.
- Commit to maintaining integrity programs to identify and combat breaches in employee integrity.

In return for participation, U. S. bound cargo gets expedited CBP processing upon arrival. [8]

C-TPAT Seeks Voluntary Private Sector Participation to Improve Cargo Container Security

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a cooperative program between CBP and members of the international trade community. Private companies agree to improve the security of their supply chains in return for a reduced likelihood that their containers will be inspected.[9]

C-TPAT membership is open to U. S.-based and foreign companies in the trade community including air/rail/truck/sea carriers, importers, licensed customs brokers, air freight consolidators and ocean transportation intermediaries, nonvessel-operating common carriers, and port authorities or terminal operators.[10]

Participation requires submission of an application including an executive summary of the company's supply chain procedures, a CBP application review, and, if approved, CBP certification. Importers undergo additional review including a separate vetting process relating to the importer's compliance with customs laws and regulations and its violation history.[11]

CBP is supposed to conduct a validation of selected certified C-TPAT members to ensure that they actually comply with the measures outlined in their security profiles.[12]

Other Well Established Federal Programs Also Regulate Intermodal Cargo Security

The Code of Federal Regulations, Title 33: Navigation and Navigable Waters provides a national framework for maritime security.

Maritime Security (MARSEC) levels, established in 33 CFR, advise the maritime community and the public of the level of risk to the maritime elements of the national transportation system. Ports, under the direction of the local Captain of the Port (an appointed U. S. Coast Guard official), will respond to changes in the MARSEC level by implementing measures specified in their local Area Maritime Security Plan.[13]

In addition, 33 CFR, Part 105 establishes a comprehensive maritime security framework for port facilities. Facilities must assign in writing a Facility Security Officer, conduct a Facility Security Assessment, and develop and submit for approval a Facility Security Plan.[14] A facility must also ensure that adequate coordination of security issues takes place between the facility and vessels that call on it.[15] Facilities are required to establish measures for access control.[16] They are required to establish security

[8] Id.
[9] GAO, *Maritime Security: Enhancements Made, But Implementation and Sustainability Remain Key Challenges*, GAO-05-448T, (Washington, D.C., May 17, 2005).
[10] GAO, *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security*, GAO-05-404, March 2005.

[11] Id.
[12] GAO, while noting continued improvement, has criticized each of the CBP programs as a result of a series of ongoing program reviews. For example, the GAO noted that CBP has not yet tested the effectiveness of ATS in targeting cargo containers for inspection but has plans to do so in the future. CSI relies on host country cooperation. From time to time, some host countries have declined to inspect containers requested by CBP officers. Further, CBP does not have sufficient staffing to properly conduct C-TPAT validations.

[13] 33 CFR, Part 101, Subpart B, s. 101.200
[14] 33 CFR, Part 105, Subpart B, s. 105.200
[15] Id.
[16] 33 CFR, Part 105, Subpart B, s. 105.255

measures to deter tampering, prevent cargo that is not meant for carriage from being accepted and stored at the facility, and establish cargo control procedures at access points to the facility.[17]

Federal regulatory authority also applies to the railroads which are a modal component of the intermodal cargo system.[18] Federal regulation places much of its focus on railroad operations and safety. However, federal law has given railroads the authority to establish their own police forces which provide another layer of security.

According to federal statute, a duly designated and commissioned railroad police officer has jurisdictional authority to enforce certain specified laws relating to railroad property in any state in which the railroad owns property. This includes laws relating to the intrastate, interstate, or foreign movement of cargo in the railroad's possession.[19]

Florida's Effort to Improve Cargo Security Preceded 9/11

Florida's cargo security role includes the establishment of security policy and standards for its public thoroughfares and ports. In addition law enforcement operations are provided by various state and local agencies.

Florida began its effort to improve cargo security at its public ports well before the attacks of September 11, 2001. The Legislature developed and passed seaport security standards to combat contraband smuggling and cargo theft during the 2000 legislative session.[20] Those standards have undergone revision and improvement several times since inception and now also reflect the need to protect Florida's ports from acts of terrorism.

The state's responsibility and involvement with intermodal cargo security generally begins landside at its public ports and extends off port to the state highway system. By agreement with DHS, Florida also provides domestic security support within the boundaries of state waters. Florida's public ports are all located within the bounds of state waters.

Florida's share of container flow through its ports in Fiscal Year (FY) 2004-2005 amounted to almost 3 million twenty-foot equivalent units (TEU).[21] The Florida Seaport Transportation and Economic Development Council forecasts this flow to grow to more than 3.7 million TEU's by FY 2009-2010.[22] Timely and efficient container handling at this volume level is essential to the state's economy.

Port officials report that a single crane operation can normally move 35 to 37 containers an hour from a container ship stack to truck transport awaiting loading dockside. Twenty-foot containers can weigh up to 52,900 lbs. and forty-foot containers an additional 14,300 lbs. or up to 67,200 lbs. Safe movement therefore requires as much precision as a choreographed ballet. Once off-loaded, containers are usually taken to staging areas on the port where they are stacked, stored, processed, and further loaded onto rail cars or over-the-road trailer chassis for delivery to their final destination.

Chapter 311, Florida Statutes (F.S.), provides for the designation of seaport security areas and access requirements to those areas.[23] The chapter establishes seaport security standards including requirements that:

- Seaport security plans be reviewed and approved by the Office of Drug Control within the Executive Office of the Governor and the Department of Law Enforcement (FDLE);
- Seaports conduct quarterly risk assessments;
- Seaports conduct fingerprint-based criminal history checks on any applicant for employment;
- Persons convicted of certain felonies within the past 7 years be denied employment or regular access to a seaport; and
- FDLE conduct no less than one annual unannounced inspection of each seaport listed in s. 311.09, F.S.[24] to test compliance with, or

[17] 33 CFR, Part 105, Subpart B, s. 105.265
[18] See Florida Senate Interim Project Report 2004-151, *Ground/Linear Transportation Security*, November 2003
[19] 49 USC 207
[20] Section 311.12, F.S.

[21] Containers come in standard lengths. A twenty foot container is considered a standard measure known as one twenty-foot equivalent unit (TEU). Forty-foot and forty-five foot containers would be measured as two TEU's.
[22] Florida Seaport Transportation and Economic Development Council, *A Five-Year Plan to Achieve the Mission of Florida's Seaports*, February 2006, page 14.
[23] Section 311.111, F.S.
[24] The ports of Jacksonville, Port Canaveral, Fort Pierce, Palm Beach, Port Everglades, Miami, Port Manatee, St. Petersburg, Tampa, Port St. Joe, Panama City, Pensacola, Key West, and Fernandina. Port St. Joe and the Port of Fort Pierce are currently considered inactive for commercial port purposes.

the effectiveness of, security plans and operations.[25]

Florida standards such as required fingerprint background checks for port employment and denial of regular port access to certain convicted felons are considered more restrictive than current federal requirements.

Florida employs executive agency law enforcement resources to aid in port and cargo security efforts throughout the state. Within the scope of their core missions, the following state agencies support domestic security missions:[26]

- Department of Agriculture and Consumer Services Office of Law Enforcement operates Agricultural Interdiction Stations which can function as control points for the interdiction of materials that could be used as weapons of mass destruction (WMD). The department possesses mobile non-intrusive inspection technology that uses gamma-ray scanning to view inside a container for anomalies. Such technology has been used in the past to assist in scanning cargo containers at ports and vehicles entering high profile security events such as the Superbowl.
- Department of Transportation Office of Motor Carrier Compliance enforces state and federal laws and agency rules that regulate the safety of commercial motor vehicles and their drivers. Motor carrier compliance officers use portable scales and fixed locations to weigh and inspect trucks for compliance with applicable laws. These officers routinely identify and interdict trucks carrying contraband.
- Fish and Wildlife Conservation Commission Law Enforcement utilizes resources provided through federal homeland security grants to assist with waterborne security patrols at ports, power plants, and military bases.
- Department of Highway Safety and Motor Vehicles Florida Highway Patrol enforces traffic laws, apprehends drivers who engage in illegal activities while on the highway, and assists other law enforcement officers on the state's highways.

Combined, these state agencies add another layer to the cargo security system.

Also railroad police officers, as mentioned previously, constitute an additional force of sworn law enforcement officers. Whether they have been sworn in Florida or in another state, railroad police are recognized in Florida as state law enforcement officers who work for private entities.[27]

Local Government and Port Operator Roles

Local government entities in Florida, primarily in the form of public port authorities, are responsible for the physical security of their respective port facilities. In some cases, port authorities are departments of county government and in others are chartered as independent entities by state law. In either case, port authorities respond to a U. S. Coast Guard Captain of the Port who holds command authority over port security and security policy. The Coast Guard supervises overall port security and conducts security operations on the water side of the port while the port authority is responsible for security on land.

Port authorities build and maintain perimeter security systems, manage port access, provide for general cargo security while located on the port, and provide for trained security personnel to conduct security operations including control of port access. These tasks are performed in close cooperation with port terminal operators and transport system entities. Port authorities regulate port tenants and users by establishing and enforcing local security rules and procedures.

Local law enforcement agencies also provide an important security function on the ports. They are an integral part of a port's security plan. They exercise normal police powers on the port, conduct roving security patrols, and provide an armed response force in the event of an attack. In addition, they play a role in local and regional efforts to combat cargo theft and interdict contraband shipments. Regional law enforcement task forces such as the Miami-Dade Police Department Cargo Theft Task Force (TOMCATS) combine the capabilities of local, state, and federal law enforcement agencies to provide another layer of cargo security.

Individual container security while on the port is the responsibility of the port terminal operator. Port terminal operators are usually private sector companies

[25] Section 311.12, F.S.

[26] Office of Program Policy Analysis and Government Accountability, Florida Government Accountability Reports (FGAR), www.oppaga.state.fl.us.

[27] Chapter 354, F.S.

in the business of loading and unloading containers, storing and processing them on the port, and transferring them to rail or motor carriers for final delivery. Once CBP releases a container for entry into the port, the port terminal operator assumes security responsibility for the container. Port terminal operators are relieved of their responsibility when the receiving rail or motor carrier accepts the container for further shipment.

Technology Is Useful But Has Its Limitations

Non-Intrusive Inspection (NII) technology in the form of x-ray and gamma-ray devices can be very effective in discovering contraband items in containers. Trained operators can easily spot items or people inside a sealed container. However, there is a perception that such devices pose a radiation risk to nearby workers' health. CBP has taken steps to accommodate such worker concerns. However, these accommodations require additional space which is often difficult to obtain on crowded ports. Furthermore, requirements to stage containers so that they can be scanned by moving the device over the container rather than driving the container through the device, consumes additional time. This can slow the flow of commerce.[28]

One proposed solution to this problem is to fit a scanner to a gantry crane lifting mechanism. Port officials reported that they were uncertain that there would be sufficient time to scan a container moving it from ship to dockside. Furthermore, stick cranes (single boom cranes) use a different method to lift containers and might not be able to accommodate a scanner device. In any case, a separate scanner operator would have to work in tandem with the crane operator at a fast pace.

The most difficult problem in employing NII devices is in determining which containers should be targeted for scanning. Ideally, only the highest risk containers are selected. However, CBP has no absolute assurance that such inspections are effective at detecting and identifying WMD.[29]

Radiation monitoring devices are available at all ports. There are generally two classes of devices, portable and fixed site. Portable radiation monitoring pagers are as small as an electronic pager or as large as a hand held two-way radio. They are hand-carried through a container storage area to check for radiation. Fixed site devices, known as radiation portal monitors, are installed at port exit gates to check containers as they exit the port. DHS has proposed installation of portal monitors at the nation's 22 largest ports.

Radiation detection devices are limited in two ways. It is uncertain whether radiation would be detected if the material is shielded. Shielding might be detected if the container is scanned by a NII device. However, not all containers are scanned. Nor does it seem possible that this will be the case in the future due to the negative impact on container traffic flow. The second limitation is false positives. Naturally occurring radiation in items such as earthen tile, kitty litter, and even persons in proximity who have recently undergone radiation therapy or certain cardiac tests can lead to a false positive. Stopping to deal with false positives also impedes the flow of container traffic.

Additional technologies are being developed and marketed to improve container security. Door and container intrusion devices can be placed inside a container before it is sealed. When a door is opened or the container interior is breached, the device sends an alert signal notifying the shipper. Such devices work better when on land and in proximity to signal receivers. At sea, such devices can be monitored by satellite but at a considerably higher cost. It is also possible that a sophisticated intruder could produce a higher power jamming signal, blocking receipt of the intrusion device's alert signal.

Standardized Credentialing Is Needed to Improve Access Control

Each public port in Florida has its own unique access credential or badge. Trucking industry officials reported that individual drivers must obtain an access badge for each port that they visit. This is both expensive and time consuming. Both the trucking industry and state government have recognized the need for a single standard badge for use at all Florida public ports.

Florida has developed such a credential known as the Florida Uniform Port Access Credential (FUPAC).[30]

[28] GAO, *Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System*, GAO-06-591T, (Washington, D.C., March 30, 2006).
[29] GAO, *Homeland Security: Key Cargo Security Programs Can Be Improved*, GAO-05-466T, (Washington, D.C., May 26, 2005).

[30] Section 311.125, F.S.

The FUPAC is in the implementation phase at the Port of Fernandina. Full roll out to all Florida ports is expected by November 2006.

The federal government requires a similar credential with its Transportation Worker Identification Credential (TWIC) program.[31] Florida has worked with DHS to develop FUPAC as a TWIC compatible system. Delays at the federal level in developing TWIC and a clear need for a credential resulted in a decision by Florida to proceed independently. It is hoped that compatibility can be achieved in the future.[32]

Congress Passed Legislation to Improve Cargo Container Security

On September 30, 2006, Congress passed the 'Port Security Improvement Act of 2006', H. R. 4954. The legislation is now pending the President's signature. It features a number of provisions aimed at improving supply chain security including:

- Establishing a revised and expedited TWIC implementation schedule.
- Establishing a voluntary long-range vessel tracking system.
- Improving maritime security command and control.
- Increasing the number of port of entry inspection officers
- Developing a strategic plan to enhance the security of the international supply chain.
- Planning and implementing improvements to the Automated Targeting System.
- Improving container standards and security verification procedures.
- Improving the Container Security Initiative.
- Prohibiting the U. S. Trade Representative from negotiating any future trade agreement that limits the Congress in its ability to restrict foreign entity operations or ownership of United States ports.

H. R. 4954 calls for 100% ATS screening of cargo containers entering the United States through a seaport and 100% scanning of containers identified as high-risk.

Conclusions for this report can be summarized as:

1. Law enforcement, port, and industry officials expressed satisfaction with the level of cooperation and information and intelligence sharing at the state and local level. While it was recognized that federal information sharing had improved somewhat, further improvement is desired.

2. Florida statute requires corporations, persons, or other business entities that employ persons to work on, or do business at seaports, regulated in s. 311.12, F.S., to notify those seaports when employees no longer should be granted access permission.[33] Evidence presented by port officials disclosed extensive failure in compliance and highlighted a need for improvement.

3. Transportation industry officials presented evidence of drivers and agents misrepresenting themselves as authorized company representatives in order to obtain access permission. This gap needs to be reviewed.

4. Committee staff observation of inspection station and port security operations highlighted the importance of highly trained and motivated law enforcement and security forces. "Street cop sense" remains an important and effective part of a layered security system.

5. An element of random checking is important to the reliability of a layered security system. Security professionals believe that terrorists are reluctant to leave shipment of WMD materials to chance. Random checks further complicate the movement of such materials and enhance the effectiveness of supply chain security. Unannounced port inspections such as those conducted by FDLE add a layer to the security system.

6. By all measures, supply chain and cargo container security has improved since September 11, 2001. However, the layered security system currently in place still has many vulnerabilities. Most of these vulnerabilities need to be addressed at the federal level. Florida, for its part, can contribute to the effectiveness of the layered security system by continuing to support the high standards set forth in Section 311.12, F.S.

[31] Public Law 107-295, Maritime Transportation Security Act of 2002.

[32] Gov. Jeb Bush letter to Sec. Michael Chertoff, (Tallahassee, FL, September 18, 2006).

[33] Section 311.125, F.S.

RECOMMENDATIONS

1. The Legislature should review s. 311.125, F.S., and determine methods to increase compliance relating to notification to seaports by employers when employee access permission is terminated.

2. The Legislature should continue to monitor development of federal government supply chain security programs and pursue opportunities to enhance the state's layered security strategy.