

# **The Subcommittee on Coast Guard and Maritime Transportation**

## **Hearing on**

### **Port Security: Credentials For Port Security**

---

#### **TABLE OF CONTENTS***(Click on Section)*

[PURPOSE](#)

[BACKGROUND](#)

[WITNESSES](#)

---

#### **PURPOSE**

The purpose of this hearing is to investigate the best way to implement a nationwide security system which requires transportation workers to hold secure identity cards. The Subcommittee will receive testimony from Administration,

transportation industry, and labor representatives.

## **BACKGROUND**

### Current Coast Guard Activities and Authorities

The U.S. Coast Guard currently has primary responsibility for the promotion of safety of life and property at sea, the enforcement of all applicable Federal laws on, under, and over the high seas and United States waters. Federal law authorizes the Coast Guard to board any vessel subject to the jurisdiction, or operation of any laws, of the United States in order to make inquiries, examinations, inspections, searches, seizures, and arrests for the violations of U.S. laws. The Coast Guard may order and force any vessel to stop and may engage in land, water, and air patrols. Federal law also authorizes the Coast Guard to control the anchorage and movement of vessels in the navigable waters of the U.S. in order to ensure the safety and security of U.S. naval vessels.

During times when the President determines that national security is endangered, the Coast Guard may seize any vessel that fails to follow its directions within U.S. territorial waters. Under the above conditions, the Coast Guard may also fine or imprison the master and crew for noncompliance with its orders as well as establish a Port Security Card Program. This program provides for the controlled access to waterfront facilities and vessels by individuals with an appropriate security background screening by the Commandant. When certain conditions exist, the Captain of the Port may be directed by the Commandant to establish a restricted waterfront area and prevent access of persons who do not hold a Port Security Card. The Coast Guard required Port Security Cards at various facilities from 1942 until the end of the Vietnam War.

In 1985, a U.S. citizen was killed during the terrorist seizure of the passenger vessel ACHILLE LAURO. In response to the vulnerability of passenger vessels and associated passenger terminals to acts of terrorism, Congress enacted the Omnibus Diplomatic Security and Antiterrorism Act of 1986. Title XI of this law constitutes the International Maritime and Port Security Act and authorizes the Coast Guard to require measures, including inspections, port and harbor patrols,

the establishment of security and safety zones, and the development of contingency plans and procedures, to prevent or respond to acts of terrorism. The law also requires that passenger vessels and passenger terminal operators develop a plan of action for implementation of security measures at the ports and passenger vessels operating from those ports. The Coast Guard must examine and approve the security plans for passenger vessels and terminals and provide oversight to ensure that the plans are being properly implemented. Passenger vessels are only allowed to embark from or disembark to terminals that hold an examined Terminal Security Plan.

Currently, the U.S. Coast Guard is enforcing a wide range of security measures on all ships entering U.S. ports. The Coast Guard has changed the 24-hour Notice of Arrival requirement for ships entering U.S. ports to 96 hours before arrival at the first U.S. port. New special rules apply for all vessels carrying dangerous cargoes and additional information is also required in the Advance Notice of Arrival. The notice must now include a listing of all persons on board, crew and passengers, with date of birth, nationality, along with the appropriate passport or mariner's document number. The Notice must also include the vessel name, country of registry, call sign, official number, the registered owner of the vessel, the operator, the name of the classification society, a general description of the cargo, and date of departure from the last port along with that port's name.

In addition, each Coast Guard Captain of the Port may employ any security measures that he deems necessary to ensure the safety and security of the port. For example, the Coast Guard has required several facilities handling dangerous cargo to provide additional security personnel and other security improvements. Facilities not addressing Coast Guard security concerns may have their operations suspended or be subjected to civil penalties.

### Issues

There are a number of issues related to creating a workable credentialing system that need to be considered. These include:

- Are different levels of "security clearances" needed, depending upon the port area in which the individual will be granted access?
- Do all ports or terminals need to have secure areas? For example, does a grain elevator or a terminal that only unloads groceries and supplies for a

- small town need to have the same level of security as an oil terminal?
- Who needs a port security card? Do truck drivers, terminal workers, railroad workers, equipment repair personnel that work at ports all need security cards? Do personnel who work only at a grain elevator terminal need security cards?
  - What is the extent of the background check for the individual? Does it include criminal acts, national driver register checks for drunk driving, drug testing, and “intelligence” checks to ensure that the individual is not a member of, or support, terrorist organizations?
  - What factors will lead to denial of a security card? What criminal actions constitute a “security risk”?

### Administration Efforts to Establish a National Transportation Worker Identification Card

At the request of the bipartisan Leadership of the House Committee on Transportation and Infrastructure and the Senate Committee on Commerce, Science, and Transportation, the Secretary of Transportation established the Credentialing Direct Action Group. This group of Administration officials is considering the possible establishment of a national transportation worker identification card to be used throughout the United States. With the increasing use of access controls in sensitive transportation facilities, many transportation workers are being forced to carry multiple types of identification cards.

The Action Group is developing a nationwide transportation worker program that:

- verifies the identity of transportation workers
- validates their background information
- assists transportation facilities with managing their security risks, and
- accounts for personnel access to transportation facilities and activities of authorized personnel.

The Action Group also intends to develop a system that:

- is fully intermodal
- minimizes the need for redundant credentials
- builds on existing technology

- minimizes the risk of unauthorized release of personal information

The Port and Maritime Security Act of 2001, S. 1214

On December 20, 2001, the Senate passed the Port and Maritime Security Act of 2001, S. 1214. Section 106 of that bill amends the Port and Waterways Safety Act (33 U.S. Code, 1226) to require employment investigations and criminal history checks of certain persons. The bill prohibits an individual from being employed in a security sensitive position at a waterfront facility if he was convicted of a specific criminal offense in the previous seven years or was released from incarceration within five years. The Secretary may allow an otherwise unqualified individual to be employed in a security sensitive position if the employer establishes alternate security arrangements acceptable to the Secretary.

**WITNESSES**

**PANEL I**

[Admiral James Underwood](#)

Director of the Office of Intelligence and Security  
Office of the Secretary of Transportation

**PANEL II**

[James M. MacDonald](#)

Vice President, Pacific Maritime Association  
representing National Association of Waterfront Employers

[Herzl S. Eisenstadt](#)

of Counsel, representing John Bowers, President  
International Longshoremen's Association

[Peter Peyton](#)

Coast Legislative Action Committee of the  
International Longshore and Warehouse Union

[Philip L. Byrd](#)

President, and CEO

Bulldog Hiway Express, Charleston, South Carolina,  
representing American Trucking Associations

DEPARTMENT OF TRANSPORTATION  
OFFICE OF INTELLIGENCE AND SECURITY  
STATEMENT OF  
REAR ADMIRAL JAMES UNDERWOOD  
ON  
SECURITY CREDENTIALS FOR PORT PERSONNEL  
BEFORE THE  
SUBCOMMITTEE ON COAST GUARD AND MARITIME  
TRANSPORTATION  
COMMITTEE ON TRANSPORTATION AND  
INFRASTRUCTURE  
U.S. HOUSE OF REPRESENTATIVES  
FEBRUARY 13, 2002

Good afternoon, Mr. Chairman and distinguished members of the Subcommittee. I want to thank you for inviting me to appear before you today to discuss the importance of security credentials for port personnel and its nexus with improving national security.

As Director, Office of Intelligence and Security and advisor to the Secretary of Transportation, I focus significant attention to land, sea and air transportation security issues as they pertain to the safety of the traveling public, movement of vital cargo to and from markets, and the preservation of the critical infrastructure that ultimately keeps the nation's economy moving.

I come before you today to discuss a very important element of security in our seaports, and for that matter, within the entire U. S. transportation system. The issue is how can we ensure that

only authorized persons gain access to transportation conveyances and to transportation facilities, including freight storage areas within seaports. The credentialing of transportation workers is but one part of a security system, and it is likely the most challenging because it raises fundamentally important concerns about individual privacy and interoperability.

In the week following the September 11th attacks, Secretary of Transportation Norman Mineta established the National Infrastructure Security Committee (NISC) to evaluate security in the surface modes of transportation and to provide recommendations for improvement.

To reach that goal, the NISC created six "Direct Action Groups" (DAGs) to examine specific modes of transportation. These included: Maritime, Hazardous Materials, Pipeline, Surface (Highways and Motor Carriers), Transit, and Rail. This, of course, followed an intensive review of aviation security.

In the past several months, the Direct Action Groups extensively interviewed industry representatives, studied transportation system vulnerabilities, and evaluated security protocols and procedures, and are now developing recommendations to improve security across the transportation network.

The Direct Action Groups reported a common concern pertaining to the need for a uniform transportation worker identification program. Pursuant to direction from the NISC, a newly formed "Credentialing Direct Action Group" (CDAG)

began examining the feasibility and process for issuing identification cards for all transportation workers and other persons who require access to secure areas at transportation facilities. Recent and pending legislation has pointed to a need for such action. Additionally the Transportation Security Administration has established a number of GO Teams that are working on various technologies and credentialing issues.

Our goal is to fashion a nationwide transportation worker identification solution that verifies the identity of transportation workers, validates their background information, assists transportation facilities in managing their security risks, and accounts for personnel access to transportation facilities and activities of authorized personnel. The Group is seeking to identify a solution that would:

- q Be fully intermodal;
- q Be built on existing technology and existing agency/industry business processes and infrastructure as much as possible;
- q Minimize the need for workers to carry multiple ID cards;
- q Ensure compliance with privacy guidelines;
- q Meet existing congressional mandates as expressed in legislation such as the Patriot Act and Aviation and Transportation Security Act; and
- q Be scaleable and expandable to address future access enabling technologies (such as biometrics, smart card and Public Key Infrastructure (PKI)).

Establishing a national transportation worker's identification solution is an immense task in many respects, depending on technology, resources and consensus. The Department of Transportation, with assistance from the General Services Administration, the Office of Personnel Management and the Department of Defense, has interacted with the broad spectrum of affected industries. Development of a feasible solution will require much more dialog with industry and examination/development of appropriate technology. Because the U.S. transportation system is so intermodal, and so dependent on foreign entities (air, truck, rail and ship), we are engaging the international community.

The immediate focus is on workers in the commercial transportation system. The Department's efforts are aimed at developing a system that would apply to any person who has unescorted access to protected areas on a transportation facility or who has access to or control of a transportation conveyance. Intended conveyances include ships/vessels, aircraft and rail conveyances that carry freight or passengers for hire, pipelines, and trucks/buses when operations require a commercial driver's license. Intended transportation facilities include those locations where passengers or freight are boarded or loaded onto a transportation conveyance or where freight is received, stored, or staged attendant to being loaded onto a transportation conveyance, including pipelines.

Authority to implement a transportation worker credentialing system was recently enhanced with the passage of Public Law 107-71 (The Aviation and Transportation Security Act). One of

the key precursors, as codified in 49 USC 114(f); specifies that the Under Secretary of Transportation for Security shall “assess threats to transportation; develop policies, strategies, and plans for dealing with threats to transportation security; ensure the adequacy of security measures for the transportation of cargo; and ensure the adequacy of security measures at airports and other transportation facilities.”

The CDAG has looked at the implementation efforts to improve security and credentialing practices at some other government agencies. The Group has consulted the GSA Smart Card Office and the Department of Defense Access Card Office for guidance on appropriate technical standards and best practices, based on their extensive work over the last several years. We are presently canvassing transportation industry partners to determine efforts underway within the transportation industry and to identify and assess technologies in use and under development and how to best incorporate these activities into our development efforts.

Our work has not yet specifically addressed issues concerning the development and maintenance costs for the system. There are significant infrastructure issues that must be addressed before we can assess what the all-inclusive costs will be.

The CDAG is working to finalize a functional requirements document, which identifies the principal attributes that a credentialing system must have to achieve the interoperability necessary to reach across the transportation industry. We have consulted with many of the major transportation labor and

industry associations, and continue this work in progress. The CDAG has held meetings that have included representatives from the transportation industry and transportation labor. A progress report briefing with industry and labor feedback was held on January 22<sup>nd</sup>. The Marine Transportation System National Advisory Council has also been briefed and given an opportunity to provide feedback on the group's efforts and recommendations. We are pleased with the level of cooperation and engagement we are receiving from maritime stakeholders.

Conceptually, thus far the most difficult issue encountered is to define the appropriate levels of security for the broad spectrum of transportation facilities and operations and how these should be applied. We are well aware there are many differences existing among transportation conveyances and facilities to be protected.

Our two recent interactions with the industry (one CDAG and one Coast Guard sponsored) have served to validate that there are immense issues before us (for both government and industry) that must be addressed in a mutually satisfactory manner if we are to affect a workable solution. The feedback received thus far is encouraging because those who have been briefed have indicated that they think this effort is headed in the right direction.

In developing recommendations for credentialing transportation workers, the effort must also consider that hundreds of thousands of foreign merchant mariners and foreign truck drivers enter the United States each year. In order to address

this in the context of credentialing, the CDAG is consulting with the Immigration and Naturalization Service.

Security credentials for port personnel is one significant element of the security system within seaports. In order for it to work effectively, there must be physical control of all access points, whether that constitutes a barrier, surveillance and interdiction program or another method of control. For all areas within a facility, access by unauthorized persons must be controlled. As well, within security sensitive areas, sufficient resources will be necessary to ensure security level access is enforced.

The Department of Transportation is presently engaged with our transportation partners on these conceptual issues, since their support will be critical. Together, we are shaping this effort for success. Our maritime borders must be thoroughly protected. Security of the United States depends on it.

Testimony of  
James M. MacDonald, Vice President, Pacific Maritime  
Association  
before the  
House Transportation and Infrastructure Committee  
Subcommittee on Coast Guard and Maritime Transportation  
Hearing on  
Port Security/Credentialing  
February 13, 2002

Good Afternoon Mr. Chairman and members of the Subcommittee, I am James M. MacDonald Vice President of Pacific Maritime Association (PMA) and Secretary to the National Maritime Safety Association (NMSA). I am here today to present the perspective of the waterfront facility operators of the PMA, the United States Maritime Alliance (USMX) and the National Association of Waterfront Employers (NAWE). I thank you for allowing me to address this Subcommittee and present our views on the various issues associated with credentialing as it relates to the very vital matter of U.S. port security.

By way of background, I have been employed by PMA for four years where I have worked to further safety (now safety and security) on the waterfront. Prior to joining PMA, I was an officer in the U.S. Coast Guard where I worked in the Marine Safety - Security and Environmental Protection Programs for thirty years. Among my assignments, I served as the Captain of the Port, Officer In Charge Marine Inspection, and Federal On Scene Coordinator in San Francisco, California, and performed

these same duties on Guam in the Marianas Islands. I also served as the Chief of the Coast Guard's Merchant Vessel Inspection Division at Coast Guard Headquarters Washington, D.C., developing policy and regulations for the safety of U.S. merchant vessels. I also was a member of the U.S. delegation to Intergovernmental Maritime Organization (IMO) in London during the development of the international double hull tanker regulations. In preparation for these duties I held several positions in operational, marine safety, environmental and training fields, often working with Coast Guard Reserve - Port Security Units (PSUs).

The principal business of the PMA is to negotiate and administer maritime labor agreements with the International Longshore and Warehouse Union (ILWU). The membership of the PMA consists of domestic carriers, international carriers and marine terminal operators doing business in California, Oregon and Washington. Because of its comprehensive membership base and the nature of many areas of its labor agreements, PMA has been and continues to play an important role in the areas of port safety and security generally.

USMX negotiates and administers the Master Labor Contract with the International Longshoremen's Association AFL-CIO (ILA) for all Atlantic and Gulf Coast ports. USMX membership consists of ocean carriers, marine terminal operators and port associations. Like the PMA, USMX is at the forefront of important maritime issues concerning safety and security.

NAWE is the national trade association representing private

sector marine terminal operators and stevedoring companies on all three coasts and the Great Lakes. NAWE members are subject to extensive federal regulation, and have been intimately involved with the development of port security legislation. NAWE worked closely with the President's Interagency Commission on Crime and Terrorism, and it presented testimony regarding port security on behalf of the industry to the Senate Commerce Committee last July.

NMSA is a national association dealing with safety matters of concern to marine terminal operators. The Association implements safety programs and procedures at marine cargo handling facilities on a multi employer basis.

Since 9/11, PMA and its members have worked closely with the Captains of the Port in California, Washington and Oregon to develop interim marine terminal security guidelines in advance of a Congressional mandate and the promulgation of formal Coast Guard regulations. These efforts were formalized by the Coast Guard through out the Coast Guard Pacific Area by PACAREA INST 16611 of January 28<sup>th</sup>. These guidelines essentially address physical port security access control and require the development of security plans. We believe these interim guidelines adequately address the elements for the physical security of marine cargo handling facilities.

I must stress that these guidelines are only interim. The industry understands that future laws and regulations will require additional or revised security undertakings. Importantly, industry understands that certain necessary security

requirements could not be implemented locally with these interim guidelines. However, the lessons learned in their development have proven invaluable to assess and improve security at our West Coast marine terminals.

Two areas of security our work groups immediately encountered that were beyond our control and that require the attention of Congress are the requirements for:

- positive identification for all persons entering marine terminals and
- positive identification of the cargo and contents of the containers entering a marine terminal.

These two elements remain as the two biggest gaps to be filled in any marine security matrix to ensure our seaports and inter-modal transportation system are safe.

Security at our seaports is a “Three Legged Stool”: one leg is physical security (the “brick and mortar” elements of fences, lighting, cameras and sensors around our terminals that define the perimeter and enable access control); the second leg is credentialing (defining and controlling who enters, exits, or remains on a marine facility and assures they have a valid reason to be there) and the final or third leg is cargo security (knowing exactly what is being brought on board a facility.)

PMA, USMX and NAWA also worked closely with the Coast Guard Headquarters at the recent regulatory workshop held in Washington D.C on January 27-28, 2002. We commend the Subcommittee’s attention to Docket USCG 01-11137 items 18-

21. These are the workgroup reports on facility security, port security, vessel security and credentialing. Indeed many of the points made in this testimony were discussed and developed at the workshop which was attended by a broad cross section of maritime industry, labor and port interests. The report from the credentialing workgroup (Docket USCG 01-11137-20) is attached for your reference.

As this Subcommittee will be holding additional hearings on cargo security, our comments at this hearing will focus on credentialing. However, it is important to note, as we found in our workgroups, physical security, credentialing and cargo security are inextricably linked. We cannot separate one element from the other in the development of our nation's security policy. None of the elements can be developed in a vacuum.

Positive Identification of persons entering a terminal facility.

While several steps may be needed as part of a long-term effort to secure the maritime transportation system, the most urgent priority is to establish control over who has access to marine terminals. In keeping with current DOT proposals, credentialing for marine terminals must be part of a larger federal process that encompasses the entire inter-modal workforce. A House Bill thus must create a uniform minimum standard for credentialing individuals who need access to a port or marine terminal facility or who have information about the contents of cargo containers or vessel movements. Today, in most major ports, there are no uniform controls over who enters the terminals, leaving these critical facilities open to those who would engage in theft, acts

of sabotage or seek to move weapons of mass destruction through the port facilities.

### One Federal Standard for Credentialing

One uniform national transportation worker ID system must be implemented - this should be based on uniform minimum standards as to what personal information is to be verified for a particular individual. This system must include the following:

- Standards must apply to all terminal workers, truckers, vendors, and others who require entry to a marine terminal facility or have access to cargo or sensitive cargo information wherever they may be in the inter-modal chain.
- All persons seeking access to marine terminal facilities (from sea or shore) must have the required national identification credential which would be used to validate identification *and* record the entry and exit to and from a waterfront facility.
- Credentials must be issued by the Federal government or appropriately delegated to a state law enforcement entity for issuance according to federal standards. Alternately, federally chartered private companies might be used. However, there cannot be different authorities in different geographic locations or states issuing credentials under different standards.
- The credentialing system must allow the facility to

control authorized access to a marine terminal facility even for credentialed individuals. The identification system must be linked to existing data bases that establish the valid business purposes that a person must have to gain access to a facility.

- Terminal and vessel employees as well as any other person required to obtain credentials must be responsible for obtaining their own credentials and ensuring that their employment screening and criminal history record check is accurate. Individuals should pay a uniform federal fee for their own credentials and required employment investigations and criminal history record checks just as an individual would pay for their own driver's license.

In short, the ID card and credentialing system in the marine and inter-modal cargo handling chain must be able to:

Authenticate the identity of all individuals seeking access to waterfront and cargo handling facilities;

Verify that individuals presenting themselves are not a risk to the facility based on security screening.

Create and maintain real time records of arrivals and departures;

Validate the business purpose for access to the facility at the time access is being sought;

Check to ensure that persons authorized to enter do not overstay the duration of the business purpose on the facility; and  
Be cost effective.

To put these requirements in context, it is instructive to look at

the West Coast experience. In the Ports of Los Angeles/Long Beach alone, longshore workers are rotationally dispatched twice a day (with additional dispatch as needed) from four different dispatch halls to potentially 46 different terminal operations. 200-400 acre terminals are the norm in Los Angeles/Long Beach, while 50-100 acre terminals are the norm further up the West Coast. Over 6.5 million TEUs (twenty foot equivalent units) of containers will move through the Ports of Los Angeles/Long Beach this year. The significant volume of waterfront traffic through the major port zones, coupled with the large number of mobile workers, presents a major challenge to implementing a positive identification card system for the waterfront.

Clearly then, the credentialing system needs to authorize individuals from a variety of sources: facility and shipping company employees, regular and temporary non-employees (e.g., contractors and consultants), visitors, vendors, truckers, rail workers, ship chandlers and agents, and official security, police or governmental agencies. To be secure, sound work practices must be in place so that operators know who is on a terminal at any time. Our industry essentially has a one door policy to our terminals. Once inside, workers and truckers have uncontrolled free access throughout the terminal. It is common to shift workers to different jobs within the terminal on the same shift. It is common that even the most junior workers have access to the vessel tied up at the facility. It is common for jobs on the terminals to be dispatched to workers of a different category (e.g. clerks jobs are sent to the longshore hall or casual hall to be filled.) It is common that in the course of their duties,

workers will have to work in all areas of a terminal. The entire terminal therefore is a security sensitive area. Thus, all persons entering the terminal must have national ID cards, and requisite employment background checks before they enter through the positive perimeter access controls. For container terminals, everyone must be treated uniformly.

The application of existing technology is essential to maximize security at waterfront facilities:

Industry faces challenges of scale that were not faced by the Coast Guard when the current Coast Guard Port Security Card Program was implemented in WWII. To put this challenge into perspective, on a busy day at one large Los Angeles terminal, over 150 company employees may be employed, over 400 ILWU workers may be dispatched and over 2500 trucks come through the gates to drop off or pick up cargo. This does not address the many vendors or ship chandlers who may arrive with their products, wares or deliveries for the vessel or terminal. However, we also have an opportunity that was not present at that time as technology has changed tremendously.

A waterfront credentialing system database needs to be, and can be, available round the clock to rapidly verify identities of ID Cardholders. It also must be able to handle large peak flows of workers who report for work prior to the shift change and truckers who arrive to pick up cargo at concentrated times during the day. As longshoremen, truckers, management staffs and other waterfront workers may travel from port to port, the credentialing system must be able to interface with multiple ports. Establishing criteria and protocols for an electronic

credentialing system that could be used at any waterfront facility along the West Coast thus is vital to addressing many of the capacity and economic issues for our industry.

Prior to 9/11 our industry was working diligently to automate and streamline steps to accept and deliver goods as quickly and efficiently as possible. That still is our goal. Now, however, we have to accomplish this within the constraints of security measures required to keep our country safe and reduce the vulnerability of our inter-modal cargo systems to criminals or terrorists. We need to be able to employ the latest technology quickly and productively to integrate positive personal identification checks as part of normal business. We also need to employ the latest technology quickly and productively to integrate positive cargo identification and control and inspection checks as part of normal business.

It is only through the comprehensive and integrated linking of technology that we can bring the enormity of the problem and the vulnerability at our marine terminals under control.

Integrated ID systems employing smart cards with biometric identification features, and other advanced technology must be used to affect a rapid, positive near real time identification.

-  
Equipment exists now to issue, link, read and record identification information. The Department of Transportation, and the Coast Guard should be able to prescribe the essential technical elements and protocols of an approved integrated identification system (much like Customs is doing with its International Trade Data System and their ACE system)

quickly. It is in fact our understanding that DOT has many Direct Action Groups (DAGs) already working on this issue. This system must be integrated with other U.S. and international transportation agencies with oversight for all inter-modal workers coming on marine terminals (i.e. FRA and FHA).

Our greatest fear, however, is that despite (or because) of the multitude of agencies, and direct action groups working on the system, we may not see a workable system and protocol for quite some time. This need not, indeed, must not be the case. The Coast Guard should have the responsibility for oversight and monitoring of these positive ID systems so that they can be quickly mandated and implemented, and if need be, private industry can be federally chartered to assist.

The systems must relate to one another:

One essential element is that these systems must be able to “talk” between the marine terminal where the person might check in and the Coast Guard and/or other federal and international law enforcement agencies. If there is a federal agency “look-out” on a particular person, authorities should know, in relative real time, if that person is on board a vessel or attempting to enter a marine terminal. As a real world example of this, after Sept 11<sup>th</sup>, PMA received an 85-page FBI look out list from MARAD attached to a Transportation Security Information Report (TSIR). It contained the names, aliases and addresses of hundreds of people of interest to the FBI. The TSIR asked that “security personnel reconcile the name list with the names on your facility’s access list.” There was, however, no practical way to manually screen the thousands of persons

entering into our terminals each day against this paper list. This must change. It can, with the introduction of existing technology.

#### Advance notice of arrival

As part of the positive identification process, no one should arrive at a marine terminal unannounced and each person should have a valid reason for being there. Just like the 96 hour notice of arrival requirement recently implemented by the Coast Guard for vessels, there should be a scheduled arrival requirement for truckers picking up or delivering cargos, contractors, employees, vendors, ship chandlers and visitors. The credentialing information should be linked in with the cargo identification information so that terminals can operate in the most efficient way.

Vessel crew lists should be provided to marine terminals in advance of the vessel arrival. Lists of ship chandlers and vendors attending specific vessels should be provided to the terminal by the agents. Service and contract vehicles and drivers should be identified prior to arrival. Terminals should also be advised in advance of the trains and their crews operating within the terminal via on dock rail.

As noted earlier, with few exceptions, longshore workers are operated on a multi-employer "hiring hall" employment basis. Longshore workers are dispatched on a daily basis to terminals each day and may work for more than one terminal on any given day or week. For the most part, individual terminal operators have no control over who is sent to work at their facilities.

Dispatch for the workers, like the truckers, must be done in advance, so terminal operators will have a complete list of who is authorized to enter their facility prior to arrival.

The advance notice requirement will result in an orderly flow of information and personnel with more time to process, scrutinize and record the identification of all persons entering marine terminals. Moreover, only bona fide, scheduled workers will be admitted to the terminals.

### Background Checks

As an integral part of improving security on our marine terminals, operators must know that persons presenting their credentials do not represent criminal or terrorist elements. Criminal background checks must be performed on all personnel seeking access to a marine terminal. Criminal background checks are the “government’s business” and should be conducted by international, federal, state or local law enforcement agencies who have access to national (and international) criminal databases. The private sector does not have the expertise or access to law enforcement databases that law enforcement agencies possess. Moreover, employers do not want access to these data bases or any of the background information. Industry only needs to know the results of the check. To ensure uniformity, any requirement for a Federal criminal background check should supercede state law. There should be an appeals procedure for people who have paid their debt to society. All the decisional or appeal procedures for background checks, including provisions for mitigation included in the Hollings Bill, should be a matter of governmental

responsibility. A House Bill should therefore require entities performing employment investigations and criminal history checks to cross check against appropriate national security data bases.

### Drug and Alcohol Testing Requirements

Marine terminal industry workers are currently exempt from federal statutory drug and alcohol testing requirements.

Congress, DOT and the Coast Guard have enacted drug and alcohol testing requirements for employees working in every other inter-modal transportation mode. Substance abuse on marine terminals is not only a health and safety concern, but compromises the integrity of waterfront security. The marine terminal link in the inter-modal chain must be covered by these existing regulations.

### Industry watchmen are not law enforcement agents:

Longshore “watchmen” are expected to do many things, but law enforcement is not one of those things. Nor should the Federal law enforcement agencies expect industry watchmen to become surrogate policemen. If a beefed up police presence is deemed necessary at any given port complex, this needs to be entirely a function of the federal government or the port authority. A House Bill must clarify that longshore employees are not to become de facto law enforcement officers.

### Conclusion:

I think we all feel the urgency of “doing something” to improve the security of our waterfront facilities. However, any steps taken, even on an interim basis, must be coordinated as part of

the bigger picture. Performing manual personal identification or cargo security checks will slow down the flow of cargo through our ports with little inherent increase in security. We need to rely on technology from the outset to connect and process the vast amounts of information. This is the most meaningful way to handle the implementation of security especially in our nation's largest ports. Better to delay to allow implementation of the right system with the right technology the first time than to implement manual controls that are not effective. Technical protocols must be uniform for interoperability. They must be designed and mandated so the system links appropriately with the facility operators as well as law enforcement. They must include security of our computer networks to protect against compromise. Finally, sufficient high-speed container screening devices need to be purchased and positioned so as not to unduly slow down commerce. In this regard, the Hollings Bill contained funding to help address building the infrastructure. I am sure this Subcommittee will address this support as well.

In summary, PMA, USMX and NAWA greatly appreciate the efforts of the United States Coast Guard and other federal and local law enforcement agencies following the terrorist attacks of September 11<sup>th</sup>. The security of our seaports is an international as well as national security issue. We must focus on awareness, preparation and prevention. PMA, USMX and NAWA member companies stand ready to work with this Subcommittee, the Secretary of Transportation and the United States Coast Guard in an effort to deter the use of our seaports as a vehicle for criminal activity or terrorist attacks – and to maintain the

viability, vitality and integrity of our marine transportation system.

**Statement of John Bowers, President  
International Longshoremen's  
Association, AFL-CIO  
to the Subcommittee on the Coast Guard and  
Maritime Transportation  
of the  
Committee on Transportation and Infrastructure  
of the  
U.S. House of Representatives  
on February 13, 2002**

To the Honorable Members of this Subcommittee:

My name is John Bowers. I am the International President of the International Longshoremen's Association, AFL-CIO, representing longshore personnel in Ports from Maine to Texas, in Puerto Rico and on the Great Lakes. In my various capacities as a leader of the ILA, also known as the I Love America Union, I am intimately familiar with the efforts of several past decades that our 65,000-plus members have played in safeguarding our nation and its interests both in times of war and peace. They have been active participants in our country's logistical lifelines and in servicing our critical international trade.

Long before the devastating events of this past September, I, along with my colleagues, responded to our government's call to take up the initiative to have the ILA's members be the "eyes and ears" on the waterfront in an effort to curtail mounting drug trafficking. Since then, our rank and file, whose family members also are affected by that and other contraband, have remained on the alert to report anything

suspicious or unusual to the proper authorities. The hazards that they confront just in their everyday occupations have now been compounded by still new forces of terrorism, which are among the concerns that this legislation timely addresses.

The ILA stands firmly behind Congress and the Administration in the effort to thwart and to defeat terrorism and other criminal acts *via* the frontline maritime gateways of our Homeland's commerce. The threats to the stability and the tranquility of the movement of ocean cargoes to their manifested destinations are as much of concern to the ILA's members and leadership as are the physical safety and security of our rank-and-file who labor daily in an already fast-moving and potentially hazardous workplace. In the aftermath of the September 11 attacks, I personally joined with representatives from the New York Shipping Association, Customs, the Coast Guard, the FBI, DOD, and the Justice Department, to discuss and plan for enhanced security for the Port of New York and New Jersey.

On behalf of all of our members, I pledge the ILA's continuing support and assistance towards protecting our ports and harbors. The ILA therefore welcomes the legislative initiatives under consideration to develop and implement meaningful port security plans which will control access to terminals and other waterfront facilities and to provide the additional funding needed for such endeavors. It applauds the inclusion of representatives of longshore and transportation labor organizations among other segments of the port community to serve on proposed local port task forces and urges our inclusion on the proposed national one as well. The breadth of our members' hands-on knowledge and experience will have much to contribute towards achieving the bill's desired objectives.

Turning to the specific subject matter of this hearing, I wish the record to reflect that the ILA is in favor of credentialing procedures for controlling access to terminals and maritime related facilities in and around U.S. ports. However that our members may take a dim view of having to everyday prove just who they are or where they can work, they know full well that the times have changed and that "business as usual" for us and the entire industry no longer can be the "norm". They recognize that the time has arrived when labor and management in the entire intermodal transportation stream, whether it be vessels, trucks, rail or air, will be subject to scrutiny and some sort of background investigations in order to make certain that individuals who cannot verify their identities and true business purposes are kept at bay.

Yet, I am obliged to point out to the members of this Subcommittee that the overwhelming majority of ILA-represented longshorepersons are hard working, responsible family members and loyal citizens. The measures that are employed to permit as well as to restrict access must be rational, both in their designs and implementations. The standards for restricting access to facilities in this as in other industries must not be crafted in terms of any prior run-ins with the law that in essence have no realistic relationship to an individual's proclivities for committing terrorism or crimes of opportunity on the waterfront. This especially is the case where the individual may have years - or even decades - of unblemished working history in the maritime workplace and in the community where he or she lives. Indeed, the teamwork that necessarily exists in the processes of loading and unloading vessels, storing and positioning cargoes and a host of other activities in a 21<sup>st</sup>

Century waterfront environment, in the interest of keeping our international trade moving as skillfully and efficiently as possible, should beckon Congress to *minimize* any potential disruptions or delays that reasonable security measures might incur. The integrity and productivity of longshore gangs are important, just as is their safety and security.

With these thoughts in mind, and keenly aware of the provisions of the companion Senate bill which provides for employment and background checks for those who have access to so-called "controlled areas" and "security-sensitive information", I urge this House, first of all, to come to grips with the realities of deepsea port operations so that our members and others who work in coastal facilities will not be needlessly impeded or prevented from performing their normal day's work, neither by reason of irrelevant prior histories nor of the locations and activities of their work. From a security standpoint area-wise, there is *no* equivalency between a container being loaded aboard or off-loaded from a vessel *and* the filling and unstuffing of a container in another area of the same terminal; just as the handling of a load of shoes is not the same as identifying and placing of a container of hazardous materials. In the final analysis, it is the susceptibility of the information, or the exploitation and exposure of the particular activity, whether to the movement of contraband, or for purposes of sabotage, or the means for terrorist acts, that must be the yardstick for accessing security-sensitive information and for designating areas for controlled access.

To the same effect, there is no good rhyme or reason to exclude an employee who, over the course of time, has shown his or her reliability as a worker *and* as a person from

access to the jobs that he or she knows and does best, by dint of an offense that may be buried in a distant past. This is particularly so where the misconduct plain-and-simple does not demonstrate an inclination - or would not raise a reasonable suspicion - for him or her to commit the sort of act that this bill is being designed to anticipate. This especially is the case when such an act would more than likely jeopardize the very individual and fellow workers.

To the extent, however, that a member of the workforce may be perceived as a security risk, I further urge a members of this Subcommittee to bear in mind that his or her livelihood - usually as a family breadwinner - is at stake and must be dealt with sensitively and fairly. The affected individual should be accorded the due process of an appeals procedure that is written into the Act, one that includes notice and access to the disqualifying information, an opportunity for a hearing, and for the introduction of evidence of mitigating circumstances that may warrant reconsideration.

In this regard, I allude to the provisions of other legislation bill pending before Congress, namely S.1750, which is a bill to make technical corrections to the hazmat provisions of the USA PATRIOT Act, which incorporates most of these protections for other workers in an inter-related segment of the transportation industry with similar stakes in their future employment. From our viewpoint, this is imperative for the evenhandedness that must be present if this legislation is to be seen as fair and consistent, not only by the affected workers but by their colleagues and by labor generally.

The investigation aspect aside, and in the same vein, labor, no less than management, deems it imperative that

the credentialing process be used for accessibility purposes only and that it inherently permit the use of means of identification, whether they be "smart cards" or other devices, with a portability feature; that is, that they can be readily used to the maximum extent feasible by the bearer from facility to facility intra-port as well as inter-port. We recognize that not all ports are organized or operate alike; yet, they nevertheless bear certain commonalities which can and should be taken into account in creating the pertinent documentation. Thus, all of the issuing authorities should use the same standards for the issuing of credentials and the essential identity elements should be universally accessible. Furthermore, it should be convenient and user friendly; and there has to be *consistent* implementation and application, so that the credentialing system does not slow down the efficient flow of commerce. The system must be able to detect invalid credentials, forestall inappropriate access to sensitive data and alert local security to suspicious individuals, for the protection of our members no less than others who work in and around our ports.

We are at one with you, DOT, the Coast Guard, Customs and all other interested government agencies in their tremendous and hopefully united effort to make our ports less vulnerable to unlawful incursions. After all, there can be no arguing with the propositions that our longest borders are our coastlines; and that the greatest volumes of international trade and traffic move through our ports. Precisely because of these factors, this Subcommittee, along with the government agencies that will be charged with implementing this legislation, should keep in mind that the major ports that are the focal points of this objective are not the only means of entry into this country that

must be sources of our concern. There likewise are numerous public and private facilities along the waterways that feed into and from - or that parallel the functions of - these ports, even if to a lesser extent, but which are equally if not more vulnerable and will assuredly be made so after the measures contemplated by this legislation are put into effect. They must not be allowed to fall between the cracks as we batten down the front doors while leaving the back doors open.

Finally, while I most certainly cannot discount this Subcommittee's concentration on the accessibility of individuals who work and transact their business in the ports, and indeed encourage its work in this regard, I must communicate my and my members' no less cogent concerns about the *accessibility of containers*, both loaded and empty, that enter these ports day in and day out.

We have been contending all along that the main vehicle for terrorizing acts, no less than for concealing and moving drugs, weapons and other contraband illegally coming over the docks, after all is said and done, is the container, of which there are annually many millions traversing terminals in each major port. I submit to the members of this Subcommittee that rather than to view longshorepersons as possible suspects, they should more meaningfully be seen as assets in complementing the objectives of this legislation. For what you really have here are over 100,000 sensitized, streetwise eyes and ears that can sense the suspicious cargoes, the irregular movements, the devious individuals who pass their way in everyday traffic. They're much like one's friendly but sometime nosy neighbors who can tell, whether instinctively or from just looking, that there is something amiss around your home or with

your lifestyle.

We perceive that the day is not far off when all of them will be required to bear seals in attesting that they have not been misused or tampered-with en route to and from the terminals. As and when that happens, it stands to reason that the maritime longshore workers who man those terminals and who are physically present to receive these containers are the most logical persons to be utilized to check on their security and proper documentation. Not only is this within their job descriptions and contractually proper; it is integral to the very work that they regularly perform on the maritime leg of the intermodal journey.

I would like to thank the members of this Subcommittee for their kind invitation and the opportunity to apprise it of the concerns of our members, whose future lives and livelihoods will be vitally affected by the course of this legislation.

**TESTIMONY OF PETER PEYTON**

**ON BEHALF OF 60,000 MEMBERS OF  
INTERNATIONAL LONGSHORE AND  
WAREHOUSE UNION**

**BEFORE THE  
COAST GUARD & MARITIME TRANSPORTATION  
SUBCOMMITTEE**

**TRANSPORTATION AND INFRASTRUCTURE  
COMMITTEE**

**UNITED STATES HOUSE OF REPRESENTATIVES**

**HEARING ON SECURITY CREDENTIALS FOR PORT  
PERSONNEL**

**FEBRUARY 13, 2002**

My name is Peter Peyton. I live and work in the adjoining ports of Los Angeles and Long Beach California, which together

constitute far and away the largest, commercial seaport area in the United States. I am equally proud to be an active member of the International Longshore and Warehouse Union (known as the "ILWU"), which since 1934 has been chosen by the thousands of West Coast port and dock workers to represent us in all matters related to our employment. Our union, the ILWU, presently represents about 60,000 working men and women, not just in the longshore and maritime industry, but also in warehouse, hotel-restaurant, health care, mining, office clerical and a variety of other industries in California, Oregon, Washington, Alaska, Hawaii and Canada.

ILWU members are proud to have the most democratic, rank-and-file controlled union in the United States and perhaps in the World. This, of course, is not by luck or accident. Union democracy, just like state democracy, requires hard work and the active, persistent and informed involvement of the members and citizens being served.

So it should not surprise you to learn that I am not an elected official of the ILWU, though I did serve one year as Vice-President of the Marine Clerks local in Los Angeles/Long Beach. On my first day as Vice-President, I called for a work stoppage because flammable liquids were being stored beside hazardous chemicals, and hazardous materials were being loaded improperly and I felt that practice jeopardized the safety and security of the workplace and the surrounding community.

Like many ILWU members, I volunteer to serve on various rank-and-file committees, which help develop the policies and

positions of the ILWU. Presently, I serve on a five member committee called the "ILWU Coast Legislative Action Committee". While we deal with all types of legislative matters affecting the longshore industry, our Committee has devoted most of its attention to seaport security issues, in general, and S. 1214, the Port and Maritime Security Act of 2001, in particular, long before the terrible events of September 11.

Before going further, I want to thank the Chairman and the entire Subcommittee for the opportunity to share with you the views of American port and dock workers concerning port security. For us, port security is not just one among many issues on the post 9-11 American agenda. For us, port security is a matter by which we, our families and our port communities live and possibly may die every single day. If you can imagine unloading thousands of containers, each filled with unknown items packed by unknown people at any and all locations throughout the world, and virtually none of these containers or ships go through any security screening before you, the longshoreman, work the ship, then you can begin to appreciate the risks and fears we face every day and understand why port security is our absolute, top concern. Working these foreign flag ships is like boarding an airplane, owned, operated and crewed by foreign nationals, a plane loaded with luggage from countless places and the luggage, for the most part, has never, ever been inspected! And all the time you wonder, will it explode? Am I being exposed to some poison or bio-weapon infecting not just me but my family, friends and neighbors? Think on that and then you can really see how vital this issue is for us. We hope you know that the members of the ILWU are committed to

making our ports and surrounding areas safe, secure, and free of criminal or terrorist activities. It is a simple matter of survival for us.

And we hope you can also appreciate that our views on port security are formed by actual, hands-on experience. We know better than just about anyone how ports and commercial docks operate and what are real, and what are imagined security problems.

It is in this context that we present our views today and urge that Congress amend S. 1214 to provide for effective, not cosmetic, security measures to protect our ports and port workers.

The basic problem with S. 1214 is that it places unwarranted suspicion and burdens on American port workers by requiring criminal background checks – checks that lack adequate due process and confidentiality protections – while providing completely inadequate measures for the inspection and screening of foreign ships, foreign crew and foreign cargo. Going back to the airplane analogy because that is something everyone in this room knows by personal experience, S. 1214 gives us whatever security and comfort you can find in having our planes handled and operated by screened workers and yet loaded with uninspected baggage. S. 1214, as currently written, gives us this type of so-called “security” for our ports. It gives us phoney rather than real port security. And it does so at the expense of American workers.

American port workers are not the enemy or the problem. After the unspeakable terrorist crimes at the World Trade Center and

the Pentagon, longshore workers have worked cooperatively with the Coast Guard and law enforcement to heighten security and to contribute to the effort to secure our ports and surrounding communities from these threats. This response, of course, is nothing new. ILWU members have always done more than their part in providing our country with highly productive and secure commercial ports in times of war and national crisis.

It is absolutely contrary to the facts and to the goal of maintaining secure seaports to treat longshore workers as security risks. Longshore workers are the front-line defense to terrorism in our ports and a critical part of the solution for keeping our ports safe and secure. It is the well-established longshore workforce that knows how things work best in the ports and, perhaps most importantly, knows who belongs where in the marine terminals. It is ILWU members who are best able to detect and report suspicious and unusual activity in the ports. The government should, therefore, enlist these dedicated workers as partners rather than as suspects in the efforts to secure our nations ports.

It is equally critical that the government not respond to the new terrorism against our country in ways that harm the productivity of our commercial seaports. Excessive or imprudent regulations that fail to account for the true realities of port operations will only result in further damage to the national and world economies, at a time when they are in perilous circumstances. We must not, through rash government regulation, accomplish the very result our enemies seek and we are trying to avoid – the disabling of waterfront commerce and elimination of our civil

liberties. Rather, the ILWU urges Congress and the Department of Transportation to devote needed funding for the development of port infrastructure to remedy port congestion. In this regard, security measures, in order to be truly effective and affordable, must be linked and developed with plans to improve port infrastructure and to relieve port congestion.

As a general matter of policy, the ILWU membership opposes background checks on any workers. During the investigation of the Interagency Commission on Seaport Security (the Graham Commission) the ILWU challenged the Commission to prove their assertion that internal conspiracies are a problem at many of our nation's ports. We asked them for an example of an internal conspiracy to commit crimes involving ILWU longshore workers. They could not produce one example of ILWU workers at our nation's ports involved in criminal conspiracies. Not one. In fact, the only involvement our members have with serious criminal activity is reporting to authorities suspicious activities and cargo. In previous testimony before the Senate Commerce, Science and Transportation Committee, we pointed out that the actions of one longshore worker at the Port of Tacoma led to the largest cocaine seizure in the Port's history.

The ILWU and its members, therefore, believe that background checks on incumbent longshoremen, who have proved their reliability as productive workers, is misguided. It should be self-evident that any disqualification or denial of waterfront employment would wrongly impose unfair penalties on the very people who have served the maritime industry and who face the greatest personal and financial risks should terrorism strike U.S

ports. In addition, disqualifying incumbent workers from their jobs, which they have successfully performed safely and securely, based on past crimes for which they have already received the legally appropriate penalties, would violate constitutional protections, including due process and the prohibitions against double jeopardy and ex post facto laws.

In Coast Guard workshops and other meetings, the industry has advocated for biometric credentials. The current Pacific Maritime Association card is biometric because it includes a photograph of the worker. The ILWU longshore caucus met last month and moved to require that every longshore worker carry this card and that the card be authenticated by a foreman prior to entering a marine facility. We do not feel the need to require that additional cards or credentials be issued to the majority of our longshore workers except for those workers who would be required to undergo background checks and security clearances . Unfortunately, we are convinced by their own statements that our employer would like to use a biometric card for purposes other than security.

The union took the step of meeting with the employers representatives, the Pacific Maritime Association, to discuss ways that management and labor could help beef up security. No commitments to enhance security were made by the employers. In fact, the union never received a response to the attached proposal.

Recognizing the strong push for background checks from various sources, we urge Congress to ensure that S. 1214

absolutely mandates certain due process and confidentiality protections and limits background checks just to those persons with security-sensitive positions. The ILWU believes that legislation introduced by Representative Corrine Brown (D-FL) wisely places limits on background checks. We also make a plea for the addition of several other provisions, such as increased inspection of containers and vessels, which are absolutely necessary for true, effective port and national security. We urge that the following be considered and adopted:

- 1) Experienced longshore workers should not be subjected to intrusive background checks. Workers with established seniority pose little, if any, risk to port security. These tenured workers have demonstrated their commitment to the safe and productive operation of their port.
- 2) At a minimum, any government background checks of port workers must be carefully tailored to accomplish the objective of promoting national and port security against terrorism. Accordingly, no worker with a past “criminal record” should be removed from any position, absent a determination, based on sufficient evidence that the individual **actually poses a security risk** with respect to potential terrorism. After all, the point of any background check is not to add new penalties for past offenses but to identify individuals who may presently pose a security risk.
- 3) Any port worker subject to disqualification or to

any limitation affecting employment must be given the right to a meaningful appeal. While S. 1214 mentions an appeal process, it does not specify the criteria and procedures to be used. Some have argued that under the current appeal provision, the only issue for review would be whether the criminal record check is accurate. This is hardly a meaningful appeal process. The provision must be clarified to ensure that the appeal review focuses on whether the individual, based on all relevant circumstances, poses a threat to port security

4) Although S. 1214 strongly suggests that criminal background checks and any resulting disqualification are limited to security-sensitive positions, additional language should be inserted to ensure that this is the case.

5) The confidentiality provisions in S. 1214 are inadequate. Given the nature and massive scope of conducting background checks on hundreds of thousands, if not millions, of people, the risk of improper disclosure and abuse in violation of privacy and other rights looms large. The Senate Bill would allow FBI and other government reports on individuals to be shared with their employers and here is where confidentiality begins to be compromised. The best way to ensure confidentiality is to limit the information given to employers and private parties. The bill should require that only the results of a check, specifically whether an individual passed or failed the background check, should

be shared with the employer. At the same time, however, the individual should be entitled to a copy of all information used in his background check, especially for purposes of a meaningful appeal.

6) Any employment security check program should apply not just to port workers, but to **all individuals, no matter their status, title or rank** in any company, who have access to secure areas in port facilities or access to cargo manifests. This would include, managers and executives in the maritime industry as well as truck drivers and vessel crew members. It is equally important for port security that all individuals, **no matter their physical location**, who have free access to cargo and ship manifests, be subject to the same background checks as port workers. It would be a major breach to the integrity of any background check program, if the thousands of employees located in offices outside port areas were excluded from such a program where they have the same, and often greater, access to manifests than do port workers.

7) Many security measures depend, in large part, on the definition of “security-sensitive positions” and “secured areas”. The findings in section 101 of the Senate Bill correctly note that security must necessarily be tailored to reflect the unique realities of each port and each port facility. So while the bill wisely does not define “security-sensitive positions” and “secured areas”, it should be amended to specify that such terms be

defined and applied by the Local Port Security Committees. It is these local committees, created in section 104 of the bill, that have the expertise and knowledge to best determine what areas and jobs need to be treated as security-sensitive.

8) As for who will serve on the Local Port Security Committees and the National Committee, we urge that the initial language in prior versions of the bill be restored to require, not just permit, that membership include representatives from private sector maritime businesses and labor organizations. Effective security measures can only be developed and implemented with the active involvement of the industries and people who are most familiar with port operations and responsible for the implementation of such measures

9) The containers on vessels and in port facilities need to be subject to some type of security screening to protect U.S. seaports and international maritime commerce. Obviously, it is both impractical and cost-prohibitive to inspect every one of the tens of thousands of containers that flow in and out of our ports each day. As an effective and fairly inexpensive alternative, the proposed legislation should at least mandate that port workers who receive containers **inspect the integrity of the outside seal** on each container, including supposedly empty containers. A broken seal would alert the port facility that the container has been tampered and that it needs to be carefully inspected before entering a facility

or being placed on a vessel. A systematic check of container seals also provides authorities with a record as to the parties responsible for placing the seal on any container that may be the means of a terrorist act.

10) Another equally necessary security measure is the mandatory inspection of so-called “empty containers”, which regularly move on and off ships each day. Many countries, including Japan, require such inspections because of the increased risk that these “empties” pose for the placement of bombs, weapons and contraband. In fact, inspection of empty containers on American docks was the customary practice up until a few years ago when companies decided it cut into profits.

11) Again, while we recognize the impracticality of inspecting every container, the legislation should at least require that cargo be fully documented and subject to on site inspection, at random, and whenever there is probable cause at the marine terminal before allowed entry. Clearly, enhanced random and for cause inspections would provide immeasurable deterrence against terrorism.

12) Legislation should require that trucks pick up and deliver cargo to secure “staging areas” at the entrance of each marine terminal to protect the terminal and the vessels from terrorist attack.

13) The legislation should require security clearance requirements for all vessels, their owners, operators and

crew before being allowed to enter a U.S. port. Presently, these vessels operate under secrecy and without regulations by the scheme of flying the flag of a country that lacks any meaningful regulations and scrutiny. The London Times has reported that the terrorist group, Al Queda, presently operates dozens of these flags of convenience vessels. This is made possible by the absence of meaningful regulation and accountability of flags of convenience vessels.

14) The legislation should require that cargo be fully documented and subject to on site inspection, for cause or at random, at the marine terminal before allowed entry.

15) It is essential that the proposed legislation be amended to specify that its provisions may **not be used in the context of any labor dispute**. Legislation addressing security concerns should not and must not be cynically used as a means to alter established federal law concerning labor-management disputes.

I appreciate the opportunity to submit comments for the record on behalf of the ILWU and our members. Let me end by saying once more that it is our deepest wish to work with Congress, the U.S. Coast Guard and our employers to make sure our nation's ports are safe and secure from terrorism as reasonably possible. I am prepared to answer any questions from Committee members.

Attachment

**ILWU PROPOSAL FOR SPECIAL CLRC MINUTES  
RE WATERFRONT  
SECURITY**

**September 20, 2001**

The CLRC met to begin assessing waterfront security issues in light of the terrorist attacks inflicted on the United States on September 11, 2001. The Coast Parties condemn these terrorist acts and will not be deterred from performing the work that is so vital to the nation's interest. Accordingly, the CLRC agreed to the following:

- 1) The Union and the Employers pledge to work together to assess the safety of waterfront personnel and the security of operations covered by the PCL&CA with respect to the threat of terrorist attacks.
  
- 2) The Union and the Employers, through the CLRC, will jointly develop any programs and initiatives that they deem appropriate in response to the threat of terrorist attacks affecting waterfront personnel and operations covered by the PCL&CA.

3) The Employers will promptly notify the Union of any developments and initiatives, including any actual or proposed government mandates, that could affect waterfront security or operations covered by the PCL&CA.

4) The CLRC will have Waterfront Security as a standing item of its regular meetings=agenda until such time as it deems appropriate.

5) The CLRC instructs all Joint Port Labor Relations Committee to review Waterfront Security as a standing item of their regular meeting's agenda and to report promptly to the CLRC any problems or proposals for its review and action.

The CLRC agreed to send copies of these minutes to all JPLRCs by facsimile today

**Testimony of  
Phil Byrd, President and CEO, Bulldog Hiway Express  
Charleston, South Carolina**

**Hearing on Port Security: Credentialing Personnel**

**Before the Subcommittee on the Coast Guard and Maritime  
Transportation  
Committee on Transportation and Infrastructure  
U.S. House of Representatives**

**Wednesday, February 13, 2002**

Good morning, Mr. Chairman and Members of the Subcommittee. My name is Phil Byrd, and I am President and Chief Executive Officer of Bulldog Hiway Express, an intermodal and truckload carrier based in Charleston, South Carolina. I am also currently serving as Chairman of the Maritime Association of the Port of Charleston. I am testifying as a member, and on behalf, of the American Trucking Associations (“ATA”), the national trade association of the trucking industry. Through its affiliated state trucking associations, affiliated conferences and other organizations, ATA represents more than 30,000 trucking companies based throughout the United States, nearly all of which face the credentialing nightmare that is becoming a reality in America’s ports. I sincerely appreciate the opportunity to speak to the Subcommittee today on the role of credentialing in security at the ports. I hope that my testimony today will convince the Subcommittee that **all criminal history record checks for**

**transportation workers should be tied to the issuance of one single, universal transportation worker security I.D. card.**

The horrifying events of September 11 have touched us all in many ways. September 11 was a tragic reminder of our Nation's vulnerability to those with evil intentions. As a result, my company and many others in the supply chain have taken a hard look at our individual practices. In addition, I am pleased that ATA has engaged a widely respected international security and anti-terrorism consultant to develop a Security and Anti-Terrorism Action Plan for the trucking industry. Our industry is serious about the security of our Nation and the goods we haul.

**Security measures taken in light of September 11 do not address the realities of the transportation supply chain.**

A sometimes unfortunate consequence of events such as September 11 is enactment of local, state, and/or federal laws and regulations that accomplish their goals, if at all, in an overly obtrusive or burdensome manner. Patterning themselves on the work of the Florida legislature with respect to the Florida seaports (which was admittedly passed before September 11), many county and state governments are considering requiring criminal history record checks and credentialing requirements on transportation workers in the supply chain – both inside and outside the ports. It is my understanding that the South Carolina and Georgia legislatures will consider legislation to require criminal history record check and credentialing requirements for the ports. Although my company does not do any business there, I am told the Port of Philadelphia requires four different I.D.'s,

and that the Ports of New York and New Jersey are considering credentialing requirements. The West Coast ports are considering similar measures.

The problem does not just lie with local and state laws and regulations. Late last year, the Senate passed S. 1214, the Port and Maritime Security Act of 2001, which contains a requirement for employment investigations and employment restrictions for security-sensitive positions but does not provide any guidance for the harmonization of standards and credentialing for those who do business at multiple ports. And a truly glaring example of a faulty law, with effect outside the ports, is Section 1012 of the USA PATRIOT Act, which was passed in the wake of September 11. Through my testimony, I intend to set forth why recent legislative and regulatory developments aimed at security do not provide an effective, long-term solution.

### The Florida example – a flawed model

Last year, the Florida legislature passed the Florida Seaport Security Act. The legislation requires each of Florida's 14 seaports to restrict access to seaports, or specific areas within the port identified as restricted access areas by the seaport's security plan, to persons who have undergone fingerprint-based criminal history checks and met the criteria for allowing access. For illustrative purposes, the Port of Jacksonville has designated the entire facility at both the Blount Island Marine Terminal and the Talleyrand Marine Terminal as "restricted" areas. The criteria for granting access is to be set by each seaport's security

plan. A person who meets the criteria for access under an individual seaport's security plan shall be granted a badge. For a trucking company operating in all 14 ports in Florida, this means that all of that company's drivers have to undergo 14 separate fingerprint-based criminal history checks using differing criteria to determine whether that driver will receive 14 separate identification badges. The cost for the criminal history check and badge for one driver is \$74 at the Port of Jacksonville, and the badge is only good for one year. Each year thereafter, the driver must undergo an additional name check with the Florida Department of Law Enforcement before being issued a badge. The cost for this check is \$25.

These are not just abstract costs. My company is now in its 53<sup>rd</sup> year of operation. We are the largest intermodal carrier operating in the Port of Charleston. We are a company-owned fleet and have roughly 200 drivers that are employees. We have done business in the Florida Ports of Miami, Tampa, and Jacksonville for years. We cannot afford to do business in these ports today. It is impossible to predict which driver will be picking up or delivering a particular load, thus we would have to pay for all 200 drivers to go through the criminal history check process three separate times. If the ports have materially different access criteria, we would have the further complexity of trying to track who is authorized to enter which port. And after all this, we still could not send a driver who has cleared background checks on three separate occasions to pick up a load at a fourth port, such as the Port of the Everglades, because the driver had not undergone that port's background check. Simply put, this situation is untenable. We no longer do business at the

Florida ports. Unfortunately, the problem is spreading.

**Security only requires one criminal history record check and the issuance of one properly designed I.D. card.**

Mr. Chairman, let me assure you that my company and my fellow ATA member companies will do what is necessary to ensure the security of our ports, our cargo, and our facilities. However, Mr. Chairman, no purpose is served by querying the same criminal history records database of the FBI 14 times for the same driver in order to gain access to the 14 ports within Florida. Nor would any purpose be served by querying the same criminal history records database of the FBI for the same driver three different times in order to gain access to ports in three different states, such as the Port of Charleston, the Port of Savannah, and the Port of Jacksonville. It should only take one check to produce the information to determine whether to issue a uniform, interoperable I.D. card that works at all the ports nationwide.

On January 22, the U.S. Department of Transportation (“DOT”) National Infrastructure Security Committee (“NISC”) Credentialing Direct Action Group (“CDAG”), a DOT-wide, multi-modal working group, briefed industry on its concept for a national transportation worker I.D. card (“TWIC”). ATA is encouraged by the initial work of the CDAG and agrees that a TWIC could be tailored to fulfill the security needs of the various modes of the transportation chain and reduce the need for redundant criminal history record checks and credentials. By leading the way in setting the standard for such a card, the DOT

appears to be providing a reasonable, practicable solution to the problems highlighted earlier in my testimony.

The TWIC concept is a far-sighted solution among a universe of narrow, provincial efforts, as typified by the Florida ports. The need for such a solution is best demonstrated by the trucking industry. A federal law requiring background checks of employees with unrestricted access to secure areas of airports has been in existence for several years. It is entirely possible that a motor carrier may pick up a load from a restricted access area of a seaport and deliver it to a restricted access area of an airport. With a properly designed TWIC, only one card would be necessary.

A properly designed TWIC will eliminate the need to bear the costs of unnecessary, duplicative criminal history record checks. A properly designed TWIC will also reduce the burden on the FBI to conduct redundant criminal history record checks. The card would have the capacity to provide additional features, as dictated by the particular mode in which the transportation worker is employed.

**Federal legislation is not compatible with the one check, one card solution.**

The Port and Maritime Security Act of 2001 (S. 1214), as passed in the Senate, contains a requirement for employment investigations and employment restrictions for security-sensitive positions. The provision contains criteria that would disqualify a person from being employed in a security-sensitive position or

having unrestricted access to controlled areas. The criteria does not match up with the criteria in the Florida legislation. The federal legislation needs to clarify that the criteria established thereunder preempts inconsistent state and local regulation. Furthermore, any federal port security measure should prescribe guidance on the issuance of an I.D. card that must be accepted by all ports nationwide. In its current state, S. 1214 could perpetuate the multiple I.D. nightmare.

As a representative of the trucking industry, I would be remiss if I did not bring up the inconsistency of the approach legislated by Congress for truck drivers with hazardous materials endorsements to their commercial driver's licenses ("CDLs") under Section 1012 of the USA PATRIOT Act and the TWIC concept being promoted by the CDAG. Section 1012 requires drivers applying for, or who already have, a hazardous materials endorsement to undergo a criminal history record check. It is as yet unclear what criteria will be used to determine whether a driver is a national security risk and thus disqualified from receiving a hazardous materials endorsement, but being subjected to another criminal history record check, whether pursuant to federal port security legislation or state port security legislation, would again be duplicative and a waste of resources. Further, under Section 1012, the motor carrier employer would never get the results of the criminal history record check. If they did get these results, as employers under S. 1214 are authorized, then a motor carrier employer could know in advance whether the driver would qualify for access to the ports.

There are some who have suggested using the CDL as the

TWIC. However, there are hundreds of thousands of transportation workers who do not possess CDLs. Further, under the USA PATRIOT Act, only those CDLs with hazardous materials endorsements will be subject to criminal history record checks. Thus, the truck driver without a hazardous materials endorsement who carries loads between seaports and airports would be subject to the same problematic, duplicative background checks currently plaguing the industry. The use of the CDL is simply not an effective long-term solution. *As a company intimately involved in the intermodal supply chain, I have to repeat again the only effective, long-term solution: all criminal history record checks for transportation workers should be tied to the issuance of one single, universal transportation worker security I.D. card.*

-

**Industry can provide an effective, long-term solution in the near future with government standards.**

Mr. Chairman, trucking wants to play a part in solving the credentialing conundrum. ATA has proposed a holistic model in which a private, government designated entity, such as ATA, would play a central role in channeling criminal history record checks for a segment of the transportation industry and issuing properly designed TWICs pursuant to government standards and guidelines. Even before September 11, many in the trucking industry placed great emphasis on pre-screening drivers. Today, this means conducting county-by-county criminal history record checks to the extent feasible and practicable. However, the trucking industry must rely on information provided by the potential employee on his/her

application for employment. The trucking industry is thus left without access to the same criminal history records that the aviation and rail sectors have, and that marine terminal operators would have under S. 1214. This lack of information limits the trucking industry's ability to effectively ensure it is putting good people behind the wheel.

Under the ATA proposal, my company could channel the fingerprints of a potential employee to the FBI through the designated entity. The government could check those prints against any database it desires, but only the results of the check against the FBI criminal history record databases would be provided to us. Based on criteria it may determine separately, the government may inform the designated entity that the entity shall not issue a TWIC security I.D. card to the potential employee. Otherwise, we, the motor carrier employer, would direct the entity to issue a TWIC security I.D. card in the name of the employee. The card would contain the employee's fingerprints and conform with DOT-prescribed software and hardware standards. The employee could then use the card to access seaports, airports, and any other areas that may restrict access for security purposes. It is a model that effectively marshals the efficiency of the private sector while preserving scarce government resources for more appropriate functions. It is also a model that could be replicated among the various segments of the transportation supply chain. For example, a singly entity in the maritime industry would act as the channeling agent to the FBI and would issue the TWIC to all qualified maritime transportation employees.

Mr. Chairman, any discussion of security in the ports also raises the issue of safety at the ports. For intermodal truckers using the seaports, the number one safety issue is roadability. Many millions of cargo-bearing containers pass through US ports every year. Whether taken directly from the port by truck or by rail, these cargo containers ultimately must be placed upon a container "chassis" to be delivered over the road by truck to the receiving customer (consignee). Unlike all commercial trucks and trailers controlled by motor carriers, chassis are supplied by steamship lines (or their agents) at ports, and are neither owned, leased or otherwise controlled by the motor carrier.

The predominantly foreign-owned steamship lines, often acting as the freight broker, control this equipment and force the motor carriers to use it as a condition of doing business with that steamship company. However, steamship lines do not conduct systematic maintenance as required by the Federal Motor Carrier Safety Regulations (FMCSRs). The reason for this is that police do not enforce the FMCSRs while the equipment rests at the ports. Except in California, police safety inspections occur outside of port facilities only after the faulty equipment has been interchanged to the trucker who is obliged to take it onto the public highways. The truckers have no authority to conduct systematic maintenance on the chassis because they do not own it, lease it, manage it, or otherwise control it. The chassis belongs to the foreign-owned steamship companies who are perfectly satisfied to watch truckers get the "tickets" at roadside inspections resulting from ocean carriers' neglect to obey the chassis safety regulations. Truckers are perfectly agreeable to be responsible for the vehicles we control and maintain as a part of

our fleet. We truckers are not willing, however, to continue allowing our safety records to be compromised by the negligence of ocean carriers or their agents. ATA requests that Congress close this public safety loophole.

## **Conclusion**

I thank your for the opportunity to testify before the Subcommittee on these important issues. When this Congress addresses security issues, it should keep in mind the realities of the transportation supply chain and take advantage of the efficiencies that industry can bring to the table. By requiring one criminal history record check and one universal security I.D. card, we can all accomplish our security and safety goals without severely disrupting the flow of commerce. The trucking industry, with the cooperation of Congress, is ready to do its part for the security of our Nation.