Ray Familathe

International Vice President

International Longshore and Warehouse Union

EXAMINING PHYSICAL SECURITY AND CYBERSECURITY AT OUR NATION'S PORTS

Committee on Homeland Security

U.S. House of Representatives

October 30, 2017

Good afternoon Chairman McCall and members of the Committee:

Thank you for inviting me to testify on the state of the physical and cyber security at our nation's ports. I am here today on behalf of the approximately 50,000 members of the International Longshore and Warehouse Union (ILWU). The ILWU represents longshore, warehouse and maritime workers in the states of California, Washington, Oregon, Alaska and Hawaii.

As a union, we have actively worked to improve port safety and to reduce the risk of terrorism at our worksites. Our members are not only among the first men and women that would be put at risk by a terrorist attack on an American port, they are also a vital component of our Country's first line of defense. Our highly skilled workers are critical to any emergency response within a West Coast port, whether it is operating cranes and heavy equipment to move vulnerable or dangerous cargo from harm's way, or contributing our know-how to containing fires and limiting release of harmful commodities. Longshore workers are in fact natural allies of law enforcement and first responders on the waterfront.

Indeed, our members include the Los Angeles Port Police, a model 125-officer force dedicated to port safety and security. This specialized police force has over 100 years of experience protecting our ports, and hosts a joint terrorism squad tasked with preventing attacks on our maritime facilities.

ILWU members also serve on the maritime security committees operated by our ports, and we strongly encourage our port industry partners to fully integrate the union into their command and control centers, including union participation in planning and emergency response drills. As a partner in port security, we not only help guard against and respond to acts of terror, but also our members are critical to assuring a rapid recovery of port operations.

Without a doubt, the ILWU takes port safety and security seriously and we strongly support programs that genuinely contribute to protecting our members and America's ports. Unfortunately, not all federal programs meet that standard. I would like to address one program that has demonstrated no effect on better securing our ports – the TWIC program. The reality is that in a modern container facility, the longshore worker has no real access to the cargo, and the documentation associated with a container's contents is not available to the worker. TWIC credentialing of longshore workers is, as a practical matter, a feel good measure promoted by those who do not understand modern container terminal operations as a way to appear to being addressing public and political concern about port security. The reality is that TWIC does nothing to mitigate the real threat – container access outside the terminal throughout the supply/transportation chain.

TWIC is also an expensive program for workers, our employers and for the federal taxpayer. An estimated 750,000 American maritime workers are covered by TWIC, at an approximate cost of $300 to $500 per person to apply for the needed credentials and renewals over 10 years. That is roughly $225 to $375 million dollars just in TWIC application costs to the industry. Just the recently issued Coast Guard rules on TWIC readers at passenger facilities alone is estimated to cost industry another $157.9 million over ten years. In addition, the federal government spends tens of millions of dollars on staffing the TWIC program, processing applications, and spot checking credentials. It has also provided millions more in port security grants to port authorities tied to the TWIC program. Yet despite the expenditure of hundreds of millions dollars on TWIC – making TWIC the maritime industry's most costly security program, eating up an enormous percentage of our limited funds for port security – no one can point to any genuine gain in the fight against terrorism. No attacks have been identified as having been deterred by TWIC. No experts cite TWIC as an impediment to potential terrorist attacks on American ports. TWIC is simply a costly failure for the industry and for the American taxpayer.

Furthermore, we are not convinced that TWIC readers will work in a maritime environment. A GAO report on the TWIC pilot program released in February 2012 concluded that "readers capable of passing all environmental tests would represent a serious business challenge to manufacture in terms of cost per unit." Further, a high number of cards malfunctioned electronically. Durability of the card is a serious issue. Sun, wind, grime, dust on cards caused fading, stained and pealing cards that have difficulty being read by TWIC readers. Further, participants in the pilot program said they would reduce the number of guards when the reader was installed – the same guards who know the names and faces of the regular workforce.

As well as being a failed security program, TWIC is a significant hardship on those 750,000 Americans who work on the waterfront. Not only is it expensive to apply for the TWIC credentials, but also the application process itself is rife with bureaucratic delays and hardships. As recently as February 2015, the TSA reported TWIC enrollment delays of more than 60 days and recommended that applicants apply for their TWICs at least 10 to 12 weeks early. Those delays occurred despite a statutory requirement to respond to the applicant within 30 days. In addition to major delays, applicants face the need for two or more in person meetings at the nearest TWIC office just to apply and later collect the credentials.

During consideration of port security legislation, the ILWU has advocated for a background check limited to "terrorism security risks," and to ensure that there is due process for workers denied a TWIC card. However, we remain concerned that in a number of instances, TWIC has been used to single out workers who may have an old felony charge in their background but do not pose a terrorism security risk.

Further, since implementation of the TWIC program, more than 50,000 workers filed for appeals after an initial TSA determination that the worker was ineligible to receive a TWIC. On an appeal, the burden is on the worker to prove that he or she was not convicted of any felony by obtaining court and police records and sending them to the TSA. TSA issues interim denials in all cases when the record on file with the FBI is an open arrest for a disqualifying offense. Even if the arrest has been dismissed by local law enforcement, local officials often fail to update this status with the FBI. In short, the FBI database is far from complete, yet TSA relies on it exclusively. Due to the large volumes, the processing of TWIC appeals and waivers at one time took over six months, during which time the worker cannot work or even obtain unemployment insurance.

At a minimum, the ILWU strongly urges this Committee to draft legislation to place the onus on TSA – not the worker – to obtain court and police records when the FBI database is incomplete. It is a considerable hardship that workers must prove they have no disqualifying convictions before obtaining a TWIC card.

Recognizing the inadequacies of this very same FBI datebase, Congress puts the burden on the FBI to fill the missing gaps when it conducts background checks for gun purchases. Why should American workers be treated more harshly when it is their very livelihoods at stake?

Another issue that should be of concern to members of this Committee, is container access outside the terminal throughout the supply/transportation chain. Prior to 9/11, ILWU marine clerks were assigned responsibility to ensure that seals on containers were not tampered with before entering the port complex, and ensuring that unsealed empty containers were not carrying contraband or even people. Cameras have replaced people to perform this function, but cameras cannot verify that seals have not been broken and resealed. Only by yanking on the seal and inspecting its integrity with human eyes can we determine if the seal has been tampered with on route. Cameras also cannot see a hidden compartment inside an empty container. We stand ready to assist in this effort if the Coast Guard decides it is a necessary component of port security**.**

In addition to recognizing the role human's play in inspecting containers, Customs and Border Protection (CBP) staffing is also critical to safe and efficient port operations. Given the enormous responsibilities of CBP – in scale and importance – Congress needs to provide a budget that puts a full roster of CBP officers on the front lines at our ports of entry. Not only are CBP officers the lead force for inspecting goods and passengers when entering the US, but at America's ports our work comes to a stop without adequate CBP staffing. Our ports cannot offer extended hours or weekend shifts to reduce freight congestion if CBP lacks officers. These officers are key to getting imports and exports efficiently and safely moving through America's ports.

The ILWU also recognizes the multiple threats presented by cyber-attacks. This includes potential hacks into public and private systems that collect TWIC data. TWIC data can reveal not only personal information, raising the risk of identity theft, but it also reveals the work patterns of thousands of waterfront employees. That is information of high value to anyone planning a terrorist attack or criminal activity at a port. It is now far easier for hostile interests to simply employ the skills of any of the tens of thousands of individuals and criminal organizations around the world with expertise in cyber-attacks than it is to invest years in trying to recruit and radicalize a random waterfront worker who only has limit access to data and cargo. We need to take port cybersecurity seriously and stop using ineffective measures like TWIC.

We would also be foolish not to acknowledge that we are at risk from cyber-attacks not just from terrorist organizations, but from hostile governments in Russia, Asia and elsewhere. In an era where wars are now often preceded or replaced by cyberattacks, ports are vulnerable. And bad actors have already shown what they can do with a cyberattack on maritime facilities.

On June 29, 2017, the *Los Angeles Times* carried this headline, "Maersk's L.A. port terminal remains closed after global cyberattack." Maersk, the world's largest shipping line was attacked in June by unknown actors with a variation on a ransomware attack called "NotPetya." This attack affected at least 17 Maersk terminals worldwide, including several along America's West Coast where the ILWU works. Maersk estimated its damages at between $200 to $300 million dollars. The Maersk terminal here in Los Angeles, the Port of Los Angeles' largest terminal in fact, was closed for days. Delays continued to ripple through Maersk's system for weeks after the attack. Operations at Maersk terminals in the Pacific Northwest return to work only because ILWU members had the know-how to temporarily return the terminal to paper-based operations.

This attack, which impacted other companies as diverse as FedEx and drug manufacturer Merck, was actually designed to destroy data files and cripple operations – not hold computer systems hostage for ransom payments. The maritime industry is considered at high risk from such attacks due to the wide spread use of older technology. This attack was so sophisticated however that it badly impacted Maersk, the company considered our industry's technology leader. If this attack had hit other major freight companies that lack Maersk's more advanced technology, the damage to port and maritime operations could have been far worse. Imagen the damage not just to our economy but to our national security if major port operations on the West Coast were brought to standstill for days at just the time America is moving critical military equipment and supplies to respond to an international crisis or when our armed forces are already in combat. We would be negligent and foolish to not assume that America's opponents – who have already launched major cyberattacks on our private and public computer systems – have not also considered this scenario.

The ILWU believes the time to comprehensively review our port cybersecurity is now. We believe it is time to review the critical dollars we are investing in port security – physical and cyber – to assure we are providing America the best protection.

Port security grants should be awarded based on their real impact on security, with an increasing priority on funding cyber security. We have enough cameras on the docks, many of which are used to monitor worker performance rather than monitoring for illegal entry. In fact, we already have over 700 cameras that are tied into the threat detection center just here at the Port of Los Angeles.

We also have enough fences paid for by US taxpayers. The Port of Stockton actually used a port security grant to place a fence in a seemingly illogical narrow space at its river port. Ironically, this fence was installed to justify allowing the workers who process fertilizer (a key component in many explosives) from not having to apply for a TWIC. Despite the objections of Congressman Jerry McNerney, the Coast Guard took no action to reverse the plan, the fence was installed making the Port's security worse – not better.

The ILWU representing the men and women who have built their careers working the waterfront, thank each of you for your commitment to our ports and we promise you have our full support in genuinely improving port security.