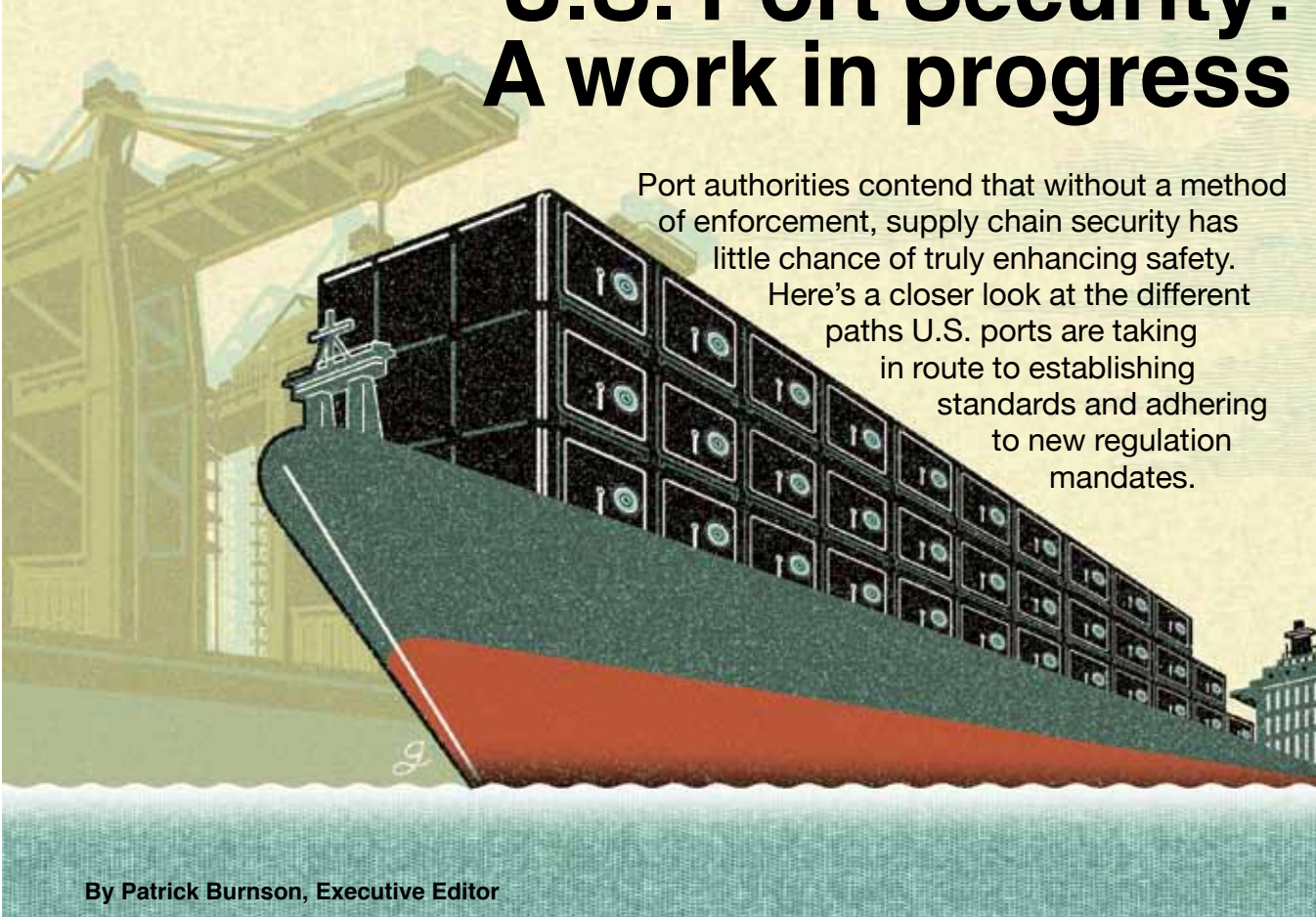


A SPECIAL SUPPLEMENT TO

# Logistics

MANAGEMENT

## U.S. Port Security: A work in progress



Port authorities contend that without a method of enforcement, supply chain security has little chance of truly enhancing safety. Here's a closer look at the different paths U.S. ports are taking in route to establishing standards and adhering to new regulation mandates.

By Patrick Burnson, Executive Editor

DANIEL GUIDERA

America's seaports are taking several different paths toward providing shippers with safe and secure commerce. And while some are more heavily reliant on sophisticated container screening systems, others are concentrating on vetting supply chain partners and intermediaries.

At the same time, all ports are mandated to comply with new U.S. regulatory rules while remaining poised to anticipate new changes in international law. Any way you slice it, security will continue to be a market differentiator and competitive tool for our ocean cargo gateways well into the future.

However, since there are an estimated 360 seaports in the U.S., no single security solution fits every gateway, says American Association of Port Authori-

ties (AAPA) spokesman Aaron Ellis. "Some ports are dealing solely with bulk and break bulk cargo, so container scanning is not going to work," he says. "And others may chiefly have roll-on/roll off and project cargo," he adds. "But for the major container ports, the standards are fairly uniform."

Joe Lawless, the Massachusetts Port Authority's (Massport) director of maritime security, agrees with Ellis, adding that 100 percent container screening will have to be customized to be effective. "Some ports will concentrate on screening for radiation, while others will place a higher emphasis concentration on routine inspection," he says. "In any case, it's one of the critical pieces that's only being worked out right now."

Lawless, who also serves as chairman of the AAPA's Port Security Committee, will be meeting with his colleagues in New Orleans this month to discuss other is-

issues related to port protection. Seaports worldwide annually handle roughly 1.5 billion tons of cargo worth more than \$1 trillion, arriving in at least 11 million containers. They require deep-water access, sufficient land for staging and storage, and unrestricted access to highway, rail, inland waterway, and pipeline networks.

At this point in time, the Department of Defense (DoD) maintains only an informal business relationship with U.S. ports. However, the DoD plays a considerable role in the security plan to prevent attacks on the ports, prepare to respond to possible attacks, and to restore their services post attack.

“But the ports themselves have to help government determine what the priorities are,” says Lawless. “That’s why AAPA members must constantly network among ourselves and our overseas counterparts to share information.”

### More fed support

The AAPA endorses the current federal strategies and supports even stronger protection measures, but not without some caveats and suggestions.

“The Port Security Grant program (PSGP) continues to be very valuable and serves as a partner with the Department of Homeland Security (DHS) to harden security at U.S. ports and to protect our homeland,” says AAPA president and CEO Curt Nagle. “But the cost must be shared.”

The PSGP funds are primarily intended to assist ports in enhancing maritime domain awareness, enhancing risk management capabilities to prevent, detect, respond to and recover from attacks involving improvised explosive devices as well as training and Transportation Worker Identification Credential (TWIC) implementation.

According to the AAPA, this can best be achieved with what it calls “Cost-share Waiver,” as ports do not have the money to contribute more than they are spending right now. Presently, says the AAPA, a 25 percent cost-share for public agencies is “a significant economic disincentive” to make security enhancements and implement regional maritime security plans.

In these tight economic times, the cost-share is an even greater problem as ports are cutting back in all areas to address economic shortfalls, authorities note. The Port Security Grant program is one of the few DHS grant programs that requires a cost-share. Transit grants and state homeland security grants, for example, are exempt from cost-share requirements.

At the same time, say port authorities, funding is key. They advocate a plan that will continue to appropriate \$400 million for the program as authorized in the SAFE Port Act. “All ports should be eligible for these funds to avoid a soft underbelly

that leaves this country vulnerable to terrorist threats,” says Nagle. “Grant funding should be better tied to port area strategic plans and funding should be made available for resiliency and business continuity projects.”

Part of this, of course, involves a quicker distribution of funds, too. Currently, there is a significant time delay between when DHS announces the awards and when FEMA finally completes all reviews and gives grantees authority to begin these security improvements. According to the ports, DHS should work to streamline their processes and get funding out more quickly.



**“Some ports will concentrate on screening for radiation, while others will place a higher emphasis concentration on routine inspection. In any case, it’s one of the critical pieces that’s only being worked out right now.”**

—Joe Lawless, director of maritime security, Massport

that leaves this country vulnerable to terrorist threats,” says Nagle. “Grant funding should be better tied to port area strategic plans and funding should be made available for resiliency and business continuity projects.”

### Command centers

Broader construction costs to improve security should be allowed if progress is to be made swiftly, according to the AAPA. “The current limits on construction projects—\$1 million or 10 percent of the total grant—should be eliminated. This is especially important for the stimulus funding, since Congress placed a priority on construction,” argues Nagle.

He further maintains that personnel costs should be an allowable expense, adding that DHS allow grant funds to be used for personnel costs, as provided in the Maritime Transportation Security Act and SAFE Port authorization legislation. This way, he says, DHS can mirror both the Urban Area Security Initiative and Transit Security Grant Programs.

In a recent statement, the AAPA urged legislators to consider allowing ports to hire new security personnel (staff for operations, fusion or emergency centers, planners, counterterrorism posts, etc.) for the term of the grant. Personnel costs, authorities further state, should also be permitted to backfill salaries for approved training programs.

Part of this manpower initiative also involves the U.S. Coast Guard. The SAFE Port Act calls for the U.S. Coast Guard to establish command centers. At the same time, some ports are developing their own centers. AAPA members argue that better coordination is needed between the Coast Guard and the Area Maritime Security Committees on the Coast Guard plans, as well as with those who are building command centers based on Port Security Grant funds.

“The U.S. Coast Guard must take a stronger role in controlling risk from small vessels that transit commercial port areas,” says Nagle. “While the Coast Guard has had several public meetings, more needs to be done to control this risk.”

### Supply chain security reality check

Is it now time for a supply chain security reality check? AAPA certainly thinks so.

## Special Report

“While the DHS has attempted to address supply chain security under the various programs that have been promulgated by Customs and Border Protection (CBP), the reality is that no internationally agreed-upon minimum supply chain security standards have been established” says Nagle.

He contends that without this global baseline and a method of either enforcement or rewards, supply chain security is largely a voluntary notion that has little chance of truly enhancing safety. Nagle and his constituents suggest that a framework for minimum mandatory supply chain security standards that is recognized and accepted worldwide is necessary in order to begin the complex process of ensuring that goods moving through the supply chain are not compromised.

According to Nagle, this framework would cover five major areas:

1. Verification that a container is free of false compartments.
2. Verification that reasonable care and due diligence has been used in packing, securing, and manifesting goods.
3. Ensuring that the cargo has not been tampered with at any point along the route.
4. Ensuring that the integrity of the information and information systems associated with movement of cargo has not been compromised.
5. Ensuring that accurate data on the shipment is provided to Customs well in advance of the ship’s arrival in the U.S.

In terms of policy, Nagle is hardly alone. Donald Masters, Ph.D., a board member of the Homeland Security Innovation Association (HLSIA), says that the U.S. should more proactively engage multilateral organizations to adopt reasonable and attainable international standards for detection equipment performance as well as procedures for their

effective use.

“The U.S.-EU Agreement calls for greater regional cooperation,” he says. “This needs to move forward with an operational protocol that specifies port requirements that meet the mutually agreed upon standards for secure transatlantic trade.”

According to Masters, a regional consensus on equipment standards and port procedures could then be expanded through the World Customs Organization. That, in turn, would make operational the already existing agreement known as the “Framework of Standards to Secure and Facilitate Global Trade.”

“Alternatively, the U.S. could make use of other regional agreements, possibly under ASEAN or APEC auspices, with major Asian trading partners,” says Masters. “Such negotiations will require patience and perseverance but if successful, they will make trading partner countries fully responsible for the safety and security of their exports.” An offshore port security system, adds Masters, would be far more cost-effective for the U.S. than the current patchwork of bilateral agreements involving the deployment of CBP teams and costly U.S. supplied equipment.

### The nuclear threat

As far as scanning equipment goes, ports are uniformly saying that CBP and the Department of Energy should work more closely with port facilities as they develop next generation detection systems. This, the ports add, would ensure that they work well with port operations.

AAPA encourages DHS to carefully evaluate the viability of the 100 percent scanning mandate and avoid instituting a system that will slow cargo movements or significantly increase the cost of shipping.

AAPA, of course, is also concerned about reciprocity. Will China, for example, require stricter standards on U.S. exports if we go too far in complicating

the supply chain?

The DHS Domestic Nuclear Detection Office has been working with ports on nuclear detection, but U.S. port authorities say more should be done to identify ways to mitigate the risk of nuclear weapons when such weapons are suspected in a shipment. As a best case scenario, DHS could work with ports on the protocols that they use and encase and shield a suspect container that is being shipped to an inspection area.

At the same time, AAPA continues to work with DHS on implementing the TWIC program, including monitoring and commenting on Coast Guard’s regulations for facility compliance with TWIC.

As the federal government seeks to apply its resources to port security issues, multiple programs and multiple agencies have become involved through homeland security programs. In order to ensure that these are adequately managing the risk associated with port security, a security system model is needed to guide its partners/stakeholders, both government and private, in the effective and efficient development and implementation of holistic port security solutions.

According to port authorities and their private sector partners, this security system model should include a coordinated approach, employee business models, and be bi-directional. Federal plans should also encourage strategic plans for port security.

“Partnering with the port industry in the development of systems-based integrated solutions, the federal government can avoid vendor-driven programs by communicating with port stakeholders from concept to execution to ensure that the dynamic needs of ports are met through a team approach,” adds Nagle. □

---

*Patrick Burnson is Executive Editor of Logistics Management*