CONTENTS

February 2013



Defense Transportation Journal

February 2013 • Vol 69, No. 1

PUBLISHER
LTG Ken Wykle, USA (Ret.)

EDITOR
Kent N. Gourdin

MANAGING EDITOR
Sharon Lo | sharon@ndtahq.com

CIRCULATION MANAGER
Leah Ashe

COPY EDITOR
Jeff Campbell

PUBLISHING OFFICE
NDTA
50 South Pickett Street, Suite 220
Alexandria, VA 22304-7296
703-751-5011 • F 703-823-8761

GRAPHIC DESIGN & PRODUCTION MANAGER
Debbie Bretches

ADVERTISING ACCOUNT MANAGER
Jim Lindsey

ADVERTISING & PRODUCTION
Carden Jennings Publishing Co., Ltd.
Custom Publishing Division
375 Greenbrier Drive, Suite 100
Charlottesville, VA 22901
434-817-2000, x261 • F 434-817-2020

CUSTOM PUBLISHING

Defense Transportation Journal (ISSN 0011-7625) is published bimonthly by the National Defense Transportation Association (NDTA), a non-profit research and educational organization; 50 South Pickett Street, Suite 220, Alexandria, VA 22304-7296, 703-751-5011. Copyright by NDTA. Periodicals postage paid at Alexandria, Virginia, and at additional mailing offices.

SUBSCRIPTION RATES: One year (six issues) $35. Two years, $55. Three years, $70. To foreign post offices, $45. Single copies, $6 plus postage. The *DTJ* is free to members. For details on membership, visit www.ndtahq.com.

POSTMASTER: Send address changes to:
Defense Transportation Journal
50 South Pickett Street, Suite 220
Alexandria, VA 22304-7296

FEATURES

DEPARTMENTS

A Department of Defense Mandate and the Global Supply Chain

By Dr. Jim Giermanski, Chairman, Powers Global Holdings, Inc.

Thank goodness for counterfeit products. Their proliferation from somewhat innocuous golf clubs, and clothing, to potentially dangerous pharmaceuticals and electronics have awakened law enforcement and finally forced a major department of government to address the issue by mandating what a contractor must do to sell a product to that department. Now, not only the exploding volume of counterfeit products coming into the United States from abroad, but also the risk connected to some of these products in failing to function or in functioning in a manner which threatens the users' health and safety have caused multiple law enforcement agencies to recognize the threat. The problem is so serious that a National Intellectual Property Rights Coordination Center (IPR Center) was created in an attempt to enforce laws regarding the importation and production of counterfeit products. The IPR is significant as indicated by its membership including the FBI, US Immigration and Customs Enforcement (ICE), Homeland Security Investigations, US Customs and Border Protection (CBP), Food and Drug Administration's Office of Criminal Investigations, US Army Criminal Investigation Command, Defense Logistics Agency (DLA), Air Force Office of Special Investigations, US Naval Criminal Investigative Service, among others.

Each has its own mission and purpose in addressing the counterfeit epidemic. However, the focus seems to be on catching and prosecuting perpetrators of counterfeit crime. There seems to be little positive or proactive steps, however, to prevent the proliferation of counterfeit products other than law enforcement and punishment. Additionally, there seems to be little attention paid to the supply chain and the control of its elements, or in mandating a process or type of technology to address the actual flow of counterfeit goods. While the players and procedures inherent in the global supply chain are many; manufacturer, shipper, carrier, movement control, consignee, and port time and control, each can be addressed and virtually secured with the use of current technology. Why, then, don't governments mandate the use of these technologies? Finally, one, the Department of Defense (DOD) has done just that. It has mandated responsibilities to contractors to address the counterfeit issue compelling them to address the role of the global supply chain in controlling the counterfeit threat. Controlling the product from origin to destination would not only protect the public, but also produce additional revenue for the controlling stakeholder.

My analysis will focus on solving some, if not most, of the vulnerabilities associated with control and movement of goods within the supply chain, specifically: verification of container contents at origin, identification of the actual person who certifies the cargo at origin, access into it throughout its movement, movement monitoring, and authorized access at destination. This is accomplished by using a chain-of-custody process that can be offered today with off-the-shelf (OTS) container security devices (CSDs).

DOD'S MANDATE

DOD has policies in place to ensure that its contractors do not sell DOD counterfeit products or products containing counterfeit components. The policies and rules are contained in the *National Defense Authorization Act (NDAA) for Fiscal Year 2012*, specifically Section 818, *Detection and Avoidance of Counterfeit Electronic Parts*. The NDAA mandates a DOD procurement policy to ensure its contractors' products are high quality, effective products that also reduce any potential harm to its military users. Those contractors who sell to DOD must make sourcing decisions "ensuring traceability of parts" (Subsection B2). Furthermore, Subsection B3 states that suppliers who fail to do "due diligence" in this regard can be suspended or debarred as a supplier. Subsection C2(A) makes contractors liable for the use of any product containing counterfeit parts. Subsection C3 states that DOD contractors and subcontractors at all levels must use "trusted suppliers" that

ensure the authenticity of the electronic parts contained in a product purchased by DOD. Furthermore, DOD contractors must use "trusted suppliers that have appropriate policies and procedures in place to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts" (Subsection 3C). Because DOD contractors assume the authenticity of their products and parts they must be able to define the standards and processes used with respect to a "trusted supplier." Other subsections require a reporting system to notify DOD of any potential counterfeit parts or shipments.

Under subsections 2(A)(B) these suppliers must establish policies and procedures to eliminate counterfeit electronic parts from the defense supply chain, which policies and procedures shall specifically address:

(i) the training of personnel;
(ii) the inspection and testing of electronic parts;
(iii) processes to abolish counterfeit parts proliferation;
(iv) mechanisms to enable traceability of parts;
(v) use of trusted suppliers;
(vi) the reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts;
(vii) methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit;
(viii) the design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts; and
(ix) the flow down of counterfeit avoidance and detection requirements to subcontractors; and
(B) establish processes for the review and approval of contractor systems for the detection and avoidance of counterfeit electronic parts and suspect counterfeit electronic parts, which processes shall be comparable to the processes established for contractor business systems.

There is also a requirement of reporting issues involving counterfeit products and the DOD contractor.

Essentially, we now have a government mandate which will force contractors dealing with DOD to use technologies and processes readily available in OTS container security products which not only protect the integrity of the container, but also provide a legal "chain of custody" providing visibility from a manufacturers' origin to the DOD user destination.

A mechanic from the 401st Army Field Support Brigade works on a vehicle at Bagram Airfield in Afghanistan. Having genuine parts is key to vehicle safety.

MEETING THE MANDATE AND INSTRUMENTS OF CONTROL: SMART CONTAINERS[1]

Counterfeit products are either surreptitiously inserted at origin, or during movement, especially in-bond movements, at transshipment ports which lack adequate security, or at the port facilities themselves. Smart containers can protect against all of these risks. The use of CSD hardware can mitigate and eliminate threats to the integrity of a shipment of products. These solutions begin at the container's stuffing, and remain through distribution to destination where the unloading is controlled. There are a number of different types of supply chain security measures that are implemented to combat counterfeiting, tampering and theft. The smartest containers offer a unique chain-of-custody process which provides for the verification of cargo by an authorized, identified person, real-time monitoring of container movement, detection, and even reporting of a container's internal environment, as well as integrity for stuffing and securing the container at origin to its opening at destination. Smart containers vary in their "smartness", some being more intelligent than others because of how they are equipped and programmed. Each type provides a different benefit for varying users.

For Department of Defense trusted suppliers, the knowledge of the electronic products used in products sold to DOD can be verified from their manufacture for inclusion in another product and the shipment of that final product in a secured, monitored shipping container anywhere in the global or domestic supply chain. These DOD shipments can be monitored for any deviation from a prescribed route of travel, called geo-fencing. For instance, a container programmed with geo-fencing detects a variance between where it should be and where it is, suggesting a hijacking, or that its being sent to the wrong consignee or the wrong location. Each benefit is programmed based on the specific needs of the shipper, carrier, or consignee. And all of the supply chain shipment data from origin to final destination will be available in servers used by the global control platforms of the CSD provider, making any required report to DOD, Customs, or other entities in the supply chain easily prepared and provided. In addition to CSD providers, there are new advances in

New shipping containers like Cakeboxx Technologies' box without doors help maintain supply chain safety.

container design and construction. For instance, Cakeboxx Technologies offers a shipping container without doors. In fact, its uniqueness and applicability of all types of cargo was highlighted by the World Customs Organization in its October 2010 edition of WCO News.

No system is 100% effective, and one cannot depend on technology alone. Because technology often overshadows the role of humans in security systems, container security systems have to include the identification of the party responsible and personally accountable for final inspection of the cargo prior to the container's sealing, dispatch and subsequent international movement to destination. Someone must necessarily be identified and responsible for confirming the cargo on the bill of lading or booking sheet, for activating the smart container system, and for sealing the container doors. This responsible party must be vetted with respect to integrity and competence. Equally, there must be a counterpart at destination. Both parties are electronically connected by a unique identifier to the smart container to complete the system. Therefore at activation, the authorized party becomes an integral element in the smart container security system, and once the container is activated by using an electronic key protocol, the identity of the authorized party who verified the cargo, electronic shipping data describing the cargo, and container number are saved and carried in the container's CSD and can be transmitted at almost any time during the container's voyage by satellite communication along with any opening of or tampering with the container, even reporting its own hijacking.

When a smart container is opened at destination by an equally accountable person and cargo is missing, or is not the cargo identified at origin and there were no breaches detected, recorded and reported, the identified person at origin who verified the cargo can face either disciplinary action, or worse, criminal action by appropriate authorities. A worldwide control centers offer the capacity to serve as a third-party electronic record of the transaction recorded automatically in its servers. Thus, smartest containers offer an electronic receipt of delivery, accomplished by the opening of the container by a person at destination who is approved and authorized to open the container, which is provided by another specialized electronic key protocol usable only with and by an authorized individual at the point of destination. In summary, a smart container provides the following benefits:

- Electronically identifies the authorized personnel stuffing and securing the container, and accepts and report information like container/trailer number, booking data;
- Carries and reports logistics data, including container number;
- Detects and reports a breach in any part of the container in real-time or close to real-time;
- Tracks the container through the supply chain;
- Identifies authorized personnel unsealing container; and
- Accommodates disparate logistics programs in communicating critical data.[2]

So far, European Datacomm (EDC), and GlobalTrak in the United States can today provide these smart containers which offer the chain-of-custody process.

WHO PAYS THE COSTS OF THE MANDATE: THERE IS NO COST

The DOD contractor can make money by using these smart containers which diminish the insertion of counterfeiting products, contamination, loss, fraud, and other supply chain inefficiencies. To show the value of container security, Customs and Border Protection (CBP) commissioned the University of Virginia to determine the cost/benefit outcome to taking security measures. Published in a 2007 cost/benefit survey report, CBP reported the following with respect to benefits of simply participating in it Customs Trade Partnership Against Terrorism (C-TPAT) program:

1. Fewer examinations (34.4% decrease)
2. Better supply chain visibility (29.4% better)
3. Predicting lead-time (24.3% better)
4. Tracking orders (22.2% better)
5. Disruptions in supply chain (28.9% fewer)[3]

Unfortunately, it seems that the return on investment (ROI) is either unknown to, unappreciated by, or not significant enough to the user, to employ smart containers. Or the user is simply focusing on the costs involved in using smart container technology, not weighing the bottom-line benefits of a visible supply chain and the automatic positive impact on counterfeiting activities and other supply-chain related costs. The NDAA mandate will force DOD suppliers to improve their bottom line if for no other reason than the positive financial impact and savings through Customs expedited treatment of containers using smart container containers as defined in the *SAFE Port Act*. The benefits of expedited shipments, alone, vary from $600 to $700 per container per move (Bearing Point Study, 2003) and $1150 per move (AT Kearney Report, 2005). Therefore, if a smart container costs you an additional $100 from origin to destination, and you save $1000 on the expedited treatment, what was the cost? Costs are associated with the loss or delay of cargo; counterfeit products; diversions; increased insurance premiums; supply chain disruptions; increased labor to reship or replace the cargo; business downtime; loss or delay in medication release; or the loss of sales. Benefits include minimizing financial risks, reduced inventory carrying costs, protection against counterfeiting; reduced or eliminate diversion costs, reduced out of stock, and reduced insurance costs.

A Stanford University recent study revealed that quantifiable benefits of security controls and technology included:

- Improved Product safety – 38% reduction in theft/loss/pilferage, 37% reduction in tampering;
- Improved Inventory management – 14% reduction in excess inventory, 12% increase in reported on-time delivery;
- Improved Supply chain visibility – 50% increase in access to supply chain data, 30% increase in timeliness of shipping information;
- Improved Product handling – 43% increase in automated handling of goods;
- Process improvements – 30% percent reduction in process deviations;
- More efficient Customs Clearance – 49% reduction in cargo delays;
- Speed Improvements – 29 % reduction in transit times;
- More Resilience – 30% improved response time; and

- Higher Customer Satisfaction – 26% reduction in customer attrition and 20% increase in new customers.[4]

Other sources offer different, but compelling, benefits to using smart container technology to include the US Congressional Budget Office, in March 2006. In a 2006 A.T. Kearney survey report, respondents stated that "…they need real-time data for accurate visibility into their supply chains."[5] The report further revealed that the US Department of Defense, itself, is now utilizing smart containers even though they are not the smartest containers. These smart boxes "…reduced overall losses (military supplies) to less than 8 percent."[6]

CONCLUSION

Using smart containers protects against insertion of counterfeit cargo during its loading at origin, during its movement, during its presence at any transshipment port, during an intended or unintended diversion, and reduces the risk of fraudulent hard documents by virtue of original electronic documents that were carried in the CSD and transmitted to control platforms to be stored in their servers. DOD's NDAA requirements may actually move the United States forward in global container security management. Certainly, the Department of Homeland Security (DHS) and CBP are not doing so. ***DTJ***

1 For an expanded treatment of smart containers, see Dr. Jim Giermanski, Smart containers: their use, their payback, WCO News, October 2009, pp. 23-25; and for an expanded technical treatment see Dr. Jim Giermanski, Container Security: Is it working?, Logistics Management, October 2009.
2 Robert W. Kelly, JD, Containing the Threat: Protecting the Global Supply Chain Through Enhanced Cargo Container Secuity, The Refore Institute, October 3, 2007, pp.8-9.
3 Abdoulaye Diop, Ph.D., David Hartman, Ph.D., Customs-Trade Partnership Against Terrorism Cost/Benefit Survey Report of Results, Weldon Cooper Center for Public Service, University of Virginia, August, 2007, p. 47.
4 Barchi Peleg-Gillae, Gauri Bhat, and Lesley Sept, Innovators in Supply Chain Security The Manufacturing Institute, Stanford University, July 2006, p. 4.
5 Smart Boxes, A.T. Kearney, July 28, 2006, p. 1.
6 Smart Boxes, A.T. Kearney, p. 2.

A confiscated counterfeit version of Cisco's Small Form-Factor Pluggable (SFP), a compact, hot-pluggable transceiver used for both telecommunication and data communications applications.

Failure of counterfeit models of the US Army's Combat Application Tourniquet, available online and on the open market, can be lethal.