U.S. Department of Homeland Security
Office of Policy
U.S Customs and Border Protection
Office of Field Operations

Action Required: Request for COAC Analysis and Input

Issue: Electronic Cargo Security Devices

Executive Summary:
DHS wishes to invite COAC to examine benefits, drawbacks, feasibility and options for the use of Electronic Cargo Security Devices (eCSDs) in supply chains. Such devices allow near real-time tracking of cargo throughout the global supply chain system, providing enhanced risk targeting, improved tracking of shipments and identification of cargo diversion, and evidence of cargo tampering. However, operational, regulatory, and policy challenges with the use of eCSDs exist.

Current Customs regulations recognize certain types of reusable eCSDs either as electronic seals on the outside of containers or as Instruments of International Traffic (IIT) when attached to or built into containers. Disposable, one-time use devices (such as Radio Frequency Identification Tags, or RFID) attached to cargo or packaging may be exempted as packaging materials. However, reusable eCSDs attached to cargo or placed inside cartons are not exempt, and require Customs entry and duty payment, complicating their use. This difference in treatment has been noted by industry, which is seeking similar treatment for the devices across all uses. Treating eCSDs as IIT will require policy and regulatory changes.

Additional study is necessary prior to such regulatory changes. DHS needs to determine the value added to cargo security by eCSDs for both the government and industry, to better understand any vulnerabilities associated with their use, and, if their use is found to be beneficial, what potential benefits would encourage adoption.

Background:
Emerging technologies are making it possible and cost effective to track cargo globally in near real time at the conveyance, container, pallet and carton level. Using local area wireless networks and global cellular telephone and satellite networks, Electronic Cargo Security Devices (eCSDs) provide location and tamper reporting. When combined with additional sensors, eCSDs may also provide other reports, e.g., radiation detection, shock/impact, etc.

Since 2013, the DHS Science and Technology Directorate (S&T) has been working with Customs and Border Protection (CBP) to evaluate reusable electronic conveyance security devices, specifically Reusable Container Security Devices (RECONS). As part of this effort, S&T established nine cooperative research and development agreements (CRADAs), resourced the National Institute of Standards and Technology (NIST) to help develop and establish guidelines and standards, began developing a cargo security data-sharing bridge between commercial industry and CBP targeting systems, and started identifying potential incentives to increase the participation of commercial shippers.

CBP and S&T also conducted operational pilots. One pilot demonstrated a cargo security technology operating in four U.S-bound supply chain routes (three truck and one rail) originating from Mexico and Canada. Another pilot involved the use of RECONs to secure containers identified for inspection during transit from the port of entry to a Centralized Examination Station (CES).

Use of eCSDs was shown to provide officers with increased decision support information at and beyond the ports of entry, better risk targeting, accurate geolocation of moving cargo, cargo diversion detection, tamper evidence, and exposure to unexpected environmental changes (e.g., shock, light, temperature, etc.). During the pilot efforts, participants experienced benefits from reduced seizures and enhanced route reporting.

The pilots and CRADA identified challenges to the use of cargo security devices:

- Data vulnerabilities. Information management is a significant challenge, both relating to the transmission/receipt and processing of data and to ensure its integrity for security purposes. In at least one instance, a pilot participant contracted a third-party data management company, resulting in potential vulnerabilities relating to employee vetting, turnover, certification, and training.
- Operational vulnerabilities. The third party firm was the link between the RECON and CBP's Automated Targeting System, but was contractually obligated to notify the participating company when conveyances were selected for inspection. From a law-enforcement perspective, this created a major vulnerability in that "spotters" would potentially be able to identify CBP targeting operations.
- Cost issues. Multiple costs are associated with the use of RECONS, including the cost of the devices themselves, the cost of cellular telephone connectivity and data, and the cost of returning the device to its point of origin after a shipment.
- Necessary regulatory changes. Currently, CBP regulations include an exception for a RECON when it is attached to or built into a container (as an Instrument of International Traffic), but not when a cargo security device is attached to or placed inside the cargo itself.

Moving Forward:
DHS recognizes international trade is expected to expand at an estimated 4 to 5 percent per year, while overall staff levels are projected to remain at current levels. This requires us to explore using technology as a staff multiplier, and a means of segmenting risk so that legitimate cargo is efficiently processed and cargo of interest selected for mitigation.

DHS is continuing to evaluate electronic cargo security devices as potentially beneficial to international supply chains. Between October 2014 and March 2015, S&T is sponsoring laboratory testing of devices at Sandia National Laboratories. The Sandia testing is focused on integration with government information systems and conducting "red team" testing. From March to September, 2015, S&T will work with the Federal Protective Service to evaluate RECON use in government-controlled supply chain. Industry input will be highly beneficial in estimated the risk, costs, and benefits associated with implementation.

DHS requests that the COAC Global Supply Chain Security Working Group consider the following questions:

- What methods of data management would be commercially feasible and cost effective while mitigating data security vulnerabilities?
- What role might third-party data management firms have, and how might employee training, vetting, turn-over, and certification issues be addressed?
- How might operational vulnerabilities be mitigated?
- What are the cost issues associated with the use of eCSDs?
- Should C-TPAT members receive additional benefits for using eCSDs and similar devices such as RECONS?
- Are other countries encouraging the use of eCSDs, and if so are there lessons learned (e.g., identified incentives/benefits) that could be used by CBP?