

CARGO SECURITY INTERNATIONAL

INTERMODAL TRANSPORT SECURITY INTELLIGENCE

www.cargosecurityinternational.com

Volume 9 Number 1 February / March 2011

GREAT EXPECTATIONS: Panama prepares for growth

Inside:

- India's Coastal Surveillance
- Spotlight on Brazil
- RFID Update
- Cargo Scanning
- Personnel Vetting
- Conference Diary

Great Expectations

Ronald Thomason of the Maritime Security Council considers how new developments in the supply chain – such as the expansion of the Panama Canal – will call for enhanced security standards

The global maritime and supply chain communities are looking forward to Panama's initiation of service through the expanded Panama Canal in 2014. The project's objective is to double the Canal's capacity to accommodate larger cargo carriers. The expectation is that the increase in capacity and reduction in transit time will result in economies of scale and cost that may be distributed to producers and consumers throughout the global supply chain. Indeed, *Moody's*, *Fitch*, and *Standard & Poor's (S&P)* have all increased Panama's sovereign rating to investment grade based, in part, on the country's ambitious infrastructure investment programme. However, the security standards and operational performance requirements for Panama in the 21st century extend beyond the Canal into the broader commercial maritime and supply chain communities.

Paradigm shift

For most of the 20th century, the focus of commercial trade and transportation operations was on operating at maximum capacity and at the lowest operating expense in order to maximise revenues. Security issues that presented challenges to that operational paradigm were handled in a reactive manner – that is, emphasis was not placed on mitigating the 'threat' until it manifested itself in such as fashion as to expose the owner/operator to a very real risk of legal or financial liability. Once the risks were identified and quantified, appropriate resources (e.g. policies, procedures, equipment, personnel and training) were deployed to 'correct' the identified deficiency.

However, while the global economies of the new millennium have brought an increased interdependence on international trade, transportation, and supply chain systems, there has also been an increase in threats directed at those systems for a variety of reasons. Criminal organisations engaged in smuggling contraband may seek to compromise the systems at points where they can surreptitiously insert their 'products' into the supply chain without detection.

'In order to achieve the desired return on the investment in Panama's trade and transportation infrastructures, the infrastructure systems must be able to operate effectively at all security levels'

Organisations with terrorist intent may seek to achieve political or economic objectives by actively or passively interrupting the flow of raw materials, finished products, or commercial activities in general. As a result, the operating paradigm for commercial trade, transportation, and supply chain operations has shifted from reactive to proactive.

The regulatory environment for trade, transportation, and supply chain operations is becoming crowded with new and overlapping security requirements and 'best practices'. These preventive security regimes identify performance objectives that address specific threats, or focus on the identification and accountability of certain dangerous chemicals, 'dual-use' materials, or other products of interest as they move through the supply chain. While regulatory instruments such as the **International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code** and the **US Maritime Transportation Security Act (MTSA)** focus on transportation sector facilities and operations, the **United Nation's (UN) Security Council's Resolution 1540**, the **International Organization for Standardization's ISO 28000 – Security Management System for the Supply Chain**, and the **US Customs**

Ronald Thomason is the Vice President of Strategic Programs for the Maritime Security Council (MSC), a not-for-profit organisation that addresses the security interests of the international maritime and supply chain communities.

Thomason is also President of Infrastructure Security Solutions LLC, a provider of security consulting services for transportation, critical infrastructure, and supply chain clients worldwide.

Contact:

Ronald Thomason
 Tel: +1 954 495 7611
 Fax: +1 704 234 2800
 Email: rjthomason
 @maritimesecurity.org

and Border Protection's (CBP) Customs-Trade Partnership Against Terrorism (C-TPAT) all seek to apply preventive security measures uniformly throughout an *entire* enterprise's supply chain. All of these programmes share similar requirements for conducting threat assessments, developing security plans, performing recurring threat and vulnerability assessments, and conducting security training and exercises for personnel at all enterprise levels. In the new millennium, an effective security programme is not limited to security management personnel but is extended to all employees across the enterprise, and includes an awareness of the preventive security postures of the company's global enterprise partners.

Security costs and benefits

Trade operations and services that are delayed or denied due to security incidents, or even credible threats of a potential incident, could effectively dilute or negate the benefits of the 'new and improved' Panama Canal. In order to achieve the desired return on investment (ROI) in Panama's trade and transportation infrastructures, the

infrastructure systems must be able to operate effectively at all security levels.

Trade operations in the commercial maritime environment are conducted at one of the three maritime security (MARSEC) levels identified in the ISPS Code and MTSA, which are generally defined as follows:

- MARSEC Level 1 – when minimum appropriate security measures shall be maintained at all times
- MARSEC Level 2 – when appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident
- MARSEC Level 3 – when further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable, imminent, or has occurred, although it may not be possible to identify the specific target.

In the pre-ISPS Code era, each country's regulatory agency responsible for compliance oversight and enforcement was limited to addressing vulnerabilities or deficiencies after they had become manifest in a manner that impacted trade and transportation operations.

'New technologies for the automated collection, analysis, and dissemination of trade and threat data will allow us to provide a measure of transparency, accountability, and security for raw materials, finished products, and other 'items of interest or concern' as they move through Panama's supply chain'



‘Implementation of a country-level security capacity programme will help Panama to establish uniform standards of practice and performance for security that will apply to the regulatory requirements across all of the applicable trade and transportation industry sectors’

Today, the many regulatory regimes that are applicable to trade and transportation have provided us with performance-based standards and practices that may be woven into an effective security blanket to protect Panama’s facilities and operations against a wide range of credible threats. In addition, new technologies for the automated collection, analysis, and dissemination of trade and threat data will allow us to provide a measure of transparency, accountability, and security for raw materials, finished products, and other ‘items of interest or concern’ as they move through Panama’s supply chain. However, in order to achieve the full benefit of these security screening, data collection, and information sharing technologies, it is recommended that a top-down programme for implementing standardised security policies and procedures for Panama’s trade and transportation system be put in place.

Country-level programme

Implementation of a country-level security capacity programme will help Panama to establish uniform standards of practice and performance for security that will apply to the regulatory requirements across all of

the applicable trade and transportation industry sectors doing business in or through Panama. Implementation of a centralised regime for compliance with the security regulations and best practices for trade and transportation community enterprises will streamline the bureaucratic and financial hurdles they are currently required to negotiate, and support the increase in trade velocity and capacity for which the expanded Panama Canal was intended.

The introduction of requirements for the integration of the security design standards and performance objectives into the design, planning, and engineering of transportation infrastructure facilities and operations will establish an operational environment that can readily support incident prevention, response and recovery, and continuity of business operations. In addition, integrating the capability for the collection and analysis of trade and security data at key links in Panama’s supply chain will support the global supply chain’s transition from a time-consuming investigative process for the identification and elimination of credible threats to commercial operations, to a compressed process where the validity, risk, and consequences of a



credible threat is identified and managed by exception.

At the moment, companies that are plugged into Panama's link in the global supply chain are taking measures individually to maintain compliance with the regulatory requirements for security to which they are subject. In some cases this has resulted in gaps in their preventive security policies and programmes resulting from dedicating limited financial resources to compliance with multiple regulatory instruments, that may not all adhere to the same metrics for the evaluation of performance, or that has not given due consideration to evolutionary changes in the security regulations. Companies engaged in all aspects of trade and transportation run the risk of exposing themselves to increased legal, financial, even criminal liability if, following a security incident, they are found to be out of compliance with the applicable security requirements. The *Deepwater Horizon* incident illustrates the potential disastrous consequences of focusing on compliance with the 'letter of the law' rather than executing 'due diligence' in ensuring 'functional compliance' with the preventive security measures which

must be adopted as a 'best business practice' by every Panamanian link in the global supply chain.

Growing responsibility

The successful opening and operation of the expanded Panama Canal will no doubt result in the desired benefits of increased capacity and decreased costs for Panama's trade, transportation, and supply chain communities. However, with increased trade velocity and capacity comes an increased responsibility for ensuring the transparency, accountability, and security of trade and transportation operations in and through Panama. Failure to maintain an operational environment in which proactive security programmes and practices are uniformly applied may result in vulnerabilities that lead to delays in transit times and increased costs.

However, by including a mechanism for the centralised collection, analysis, and dissemination of trade and threat data necessary to ensure transparency, accountability, and the security of commercial trade, Panama can solidify its role as the strongest link in the supply chain serving the Western Hemisphere and the world.

'By including a mechanism for the centralised collection, analysis, and dissemination of trade and threat data necessary to ensure transparency, accountability, and the security of commercial trade, Panama can solidify its role as the strongest link in the supply chain serving the Western Hemisphere and the world'

