



Cargo Security White Paper

Prepared by PricewaterhouseCoopers LLP



Cargo Security White Paper

Independent Verification of
C-TPAT Cargo Security Controls

PricewaterhouseCoopers

May 26, 2005

“Trust, but verify” — President Ronald Reagan

A private sector, third-party verification process has been successful in several government policy initiatives. This white paper proposes a similar solution to reduce the risk that terrorists will exploit legitimate trade and the intermodal container to attack the United States using a weapon of mass destruction. By embedding a private sector, third-party verification process in the Customs-Trade Partnership Against Terrorism (C-TPAT) program, the United States can better protect and expedite the transport of cargo through its ports.

The supply chains carrying goods vital to the US economy and way of life must be secure against threats. This security includes the nation's shipping ports and the intermodal containers used to transport most products. A terrorist incident involving a weapon of mass destruction shipped into the United States within an intermodal container could cause significant economic consequences.

Besides the potential loss of life and property from a terrorist incident, a loss of public confidence in border security resulting in the closure of ports and land crossings would have a devastating ripple effect on the US economy. The potential impact is broad and deep, given the dynamic relationships among ports, border operations, carriers, supply chains, producers, and consumers. The port industry and port users generate nearly 16 million jobs and handle more than \$2 trillion worth of international trade annually, accounting for 27 percent of the United States' gross national product (GNP).¹ US Coast Guard officials believe that the closure of a single major port for just one month because of a terrorist attack could cost the United States \$60 billion in economic losses.

In the aftermath of 9/11, the US government developed cargo container initiatives to help protect the nation's ports and supply chains. Important elements in the US Customs and Border Protection (CBP) cargo security strategy are the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT), and C-TPAT Plus. These programs depend on private sector voluntary compliance.

However, the C-TPAT and C-TPAT Plus programs will also require massive efforts for companies to obtain and maintain validation status, let alone verification of security processes. C-TPAT, for example, currently has more than 7,000 participants and, so far, a little over 700 have been validated. The government currently lacks the resources to perform all of the required validation. Relying solely on supply chain participants to perform self-assessments could be a lengthy process, and a tragic event could occur in the meantime. A significant opportunity exists to use the expertise of thousands of supply chain and verification specialists who can help companies prepare and comply with new security standards. PricewaterhouseCoopers proposes that a private sector, independent third-party verification process be integrated into the C-TPAT and C-TPAT Plus programs.

¹ Comments by Kurt Nagle, President, American Association of Port Authorities.

Current Cargo Security Initiatives

CBP's Container Security Initiative (CSI) and Customs-Trade Partnership Against Terrorism (C-TPAT) form the core of CBP's cargo security program. Other important CBP security efforts include increased random inspections, enhanced use of technology, accelerated R&D spending on improved security, tracking and inspection technology, the development of ship and port security requirements, and pre-arrival boardings of cargo ships by the US Coast Guard.

Container Security Initiative

CSI is a program in which intelligence is used to target shipments for enhanced inspection, usually at foreign ports before being loaded on ships bound for the United States. This system depends on private sector cooperation to provide a detailed and accurate advance cargo manifest that accompanies the shipment. A 24-hour rule dictates that this manifest be submitted 24 hours before loading. If the information in the documents contains obvious discrepancies, triggers any intelligence red flags, or otherwise raises suspicions, the container is held until all questions are resolved. CBP generally uses traditional enforcement mechanisms to resolve any inaccuracies or falsifications in the paperwork, but these actions usually occur long after the cargo has arrived at its destination. The private sector's role in ensuring that the shipping documents are correct is thus critical to the success of CSI.

Customs-Trade Partnership Against Terrorism

C-TPAT is a voluntary government and private sector partnership program based on self-verification for compliance. Participants in C-TPAT attest to the integrity of their security practices and communicate their security guidelines to their business partners within the supply chain. Participants will sign an agreement that commits them to the following actions:

- Conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines jointly developed by CBP and the trade community. These guidelines encompass the following areas: procedural security, physical security, personnel security, education and training, access controls, manifest procedures, and conveyance security.
- Submit a supply chain security profile questionnaire to CBP.
- Develop and implement a program to enhance security throughout the supply chain in accordance with C-TPAT guidelines.
- Communicate C-TPAT guidelines to other companies in the supply chain and work to build the guidelines into relationships with these companies.²

Once CBP has approved C-TPAT participants, they can expect fewer inspections on their shipments and other benefits to expedite cargo movement.

² US Customs & Border Protection, "C-TPAT Fact Sheet and Frequently Asked Questions," http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/fact_sheet.xml.

The foundation of the C-TPAT system is a voluntary process that has self-policing and self-assessment as its goals.³ Although the published guidelines for the program are written in very general terms, approval for participation is by no means *pro forma*. C-TPAT participants must develop a detailed security profile. In the validation process, CBP and a representative of the C-TPAT participant review that profile to make sure the participant is performing the security actions detailed in the profile. This validation appears to be primarily a paper review and does not involve unannounced visits.⁴

The C-TPAT Plus program, announced in early 2005, offers even greater incentives to participants that implement stricter security measures in their supply chain. These participants would receive “green lane” status, allowing their shipments to pass through without inspections.

Theories of Regulation

The C-TPAT program implicitly leverages some of the extensive academic theory and research on achieving high levels of compliance with governmental regulation. C-TPAT, however, also emphasizes incentives: speedier processing through customs. C-TPAT certification reduces the probability of physical inspection and C-TPAT Plus certification would require no inspections at all. Because the threat of terrorists impacting the US supply chains is evolving, cargo security programs can benefit from the experience of other regulatory systems.

These systems of regulations and compliance incentives have developed over many decades, leading to best practices for facilitating commerce while protecting society from intentional or unintentional injury. Broad swaths of industry including financial services, chemicals, forestry, food and agriculture, and pharmaceuticals have interacted with governments and regulators, producing empirical outcomes that allow the measurement and improvement of regulatory schemes. Researchers have generated useful frameworks within which the challenges of protecting ports and supply chains from terrorist incidents can be examined and informed, making greater security possible. At the same time, special circumstances may be associated with securing the global supply chain that exceed previous regulatory and compliance regimens and prompt the consideration of new ideas and approaches.

Theories of regulation focus on a number of different parameters. CBP’s primary concern is for logistics providers and manufacturers to achieve high rates of compliance with C-TPAT guidelines and regulations. A second major concern is to achieve high compliance cost-effectively and with minimal impact on commerce.

³ US Customs & Border Protection, “C-TPAT Validation Process Guidelines.” http://www.cbp.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/validation_process_guidelines.ctt/validation_process_guidelines.pdf.

⁴ US Customs & Border Protection, “C-TPAT Validation Process Guidelines.” http://www.cbp.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/validation_process_guidelines.ctt/validation_process_guidelines.pdf.

Motivation for Compliance

In *Responsive Regulation*,⁵ Ayers and Braithwaite reviewed regulatory, compliance, and enforcement schemes across several industries. They described a dichotomy where governments tended to achieve compliance with regulations either through strong, punitive enforcement at one extreme, or through weak, cooperative persuasion at the other. These solutions tend to create tensions that result in pendulum swings between the end points. Ayers and Braithwaite proposed that cost-effective, efficient compliance is best achieved by developing a compliance pyramid that encourages voluntary actions by the regulated entities, while making very public the escalation process that noncompliance will inevitably entail.

New Zealand's Inland Revenue Service has used this model to achieve higher rates of compliance with tax filing laws and regulations. Figure 1 illustrates Inland Revenue's conceptualization of the pyramid and approach to enforcement.

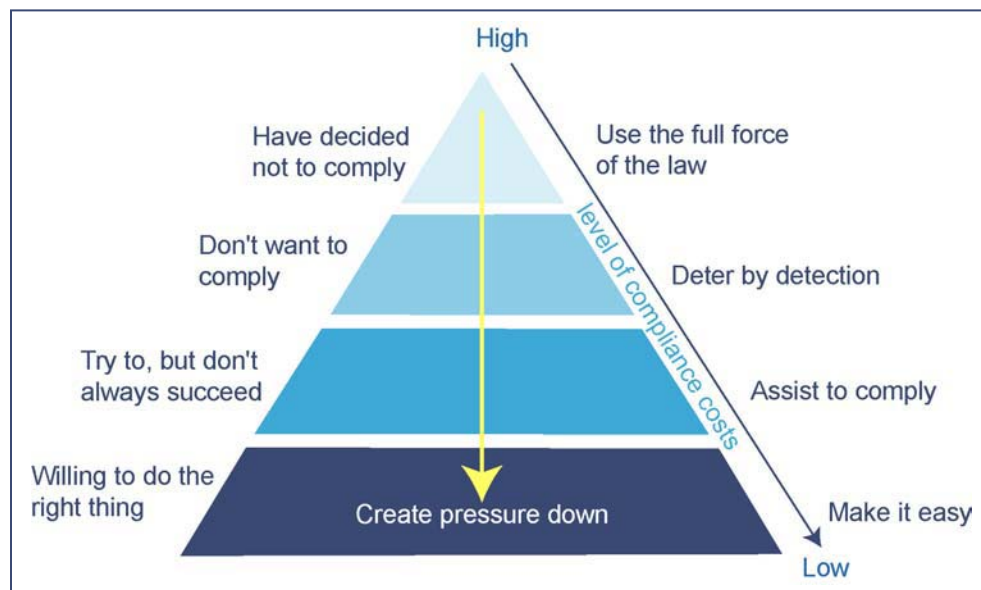


Figure 1: New Zealand's Tax Compliance Model

Key points to this approach include:

- A variety of pressures, including social and financial, impel individuals to comply.
- Most will want to comply if it is made easy to do so.
- Some will not be able to comply without assistance, even if their intent is to do so.
- A detection scheme must be deployed to identify any failure to comply, and noncompliance must be made public knowledge.
- Ultimately only a small percentage will still decide not to comply, allowing the agency to focus its resources on that small minority for enhanced detection and prosecution.

⁵ Ian Ayers and John Braithwaite, *Responsive Regulation*, (Oxford University Press, 1992).

CBP and the C-TPAT program recognize that most supply chain participants want to comply and that many need assistance to achieve compliance. Because 7,400 companies are enrolled in C-TPAT and CBP has less than 100 supply chain specialists on staff, the vast majority of supply chain participants have little fear of detection if their cargo security processes are defective. In addition, while the incentives for compliance are clear, the penalties for noncompliance are less so.

Even if CBP had a clearly defined and publicized compliance pyramid framework, noncompliance may remain a significant problem, especially when an industry program such as C-TPAT brings economic benefit through self-verified compliance. A 2003 study by Lenox and Nash⁶ examined companies' compliance with health and safety codes of practice in four separate trade associations.⁷ Some trade associations issued compliance certifications to their members only where compliance was verified by external third parties. Others allowed their member companies to self-verify their compliance to codes of practice. By using empirical measures of pollution and other parameters, Lenox and Nash demonstrated a clear impact of third-party verification: Companies in trade associations not requiring third-party verification polluted more. This finding indicates that self-verification failed to achieve the direct goal of less pollution and implies that their compliance with codes of practice was inferior.

Clearly, the “threat of detection” is required to keep some companies in full compliance with regulations. Given the limited number of CBP inspectors on staff, a program of verification using third-party auditors is necessary for the regulation and compliance pyramid to work.

Structure of Regulation

Developing a compliance pyramid is the element that leads to high levels of regulatory compliance at an affordable cost. Designing a structure of regulation for many different industries and issues is yet another concern. Historically, regulators have focused on one of two structures:

- **Performance-based regulation**—Focuses on directing companies to achieve certain standards of outcome, such as not releasing toxic chemicals into the atmosphere, or maintaining bacteria levels below a prescribed level in food and drink products.
- **Technology-based regulation**—Focuses on the processes that are, for example, involved in the manufacture of products and services, where the regulator has good reasons to believe that following certain procedures will achieve the desired outcomes.

A recent study by Coglianesi and Lazer⁸ described a third structure called management-based regulation. This type of regulation is most applicable where the complexity of

⁶ “Industry Self-Regulation and Adverse Selection: A Comparison Across Four Trade Association Programs,” *Business Strategy and the Environment*, V12, (2003).

⁷ American Chemistry Council, National Association of Chemical Distributors, American Textile Manufacturers Institute, American Forest and Paper Association.

⁸ *Management-Based Regulation: Prescribing Private Management to Achieve Public Goals*, Regulatory Policy Program, Center for Business and Government, John F. Kennedy School of Government, Harvard University, (2002).

industrial processes defy easy prescription (technology-based) and where measuring outputs is complicated (performance-based). Figure 2 shows a framework that Coglianese and Lazer suggest for determining when management-based regulation is most appropriate.

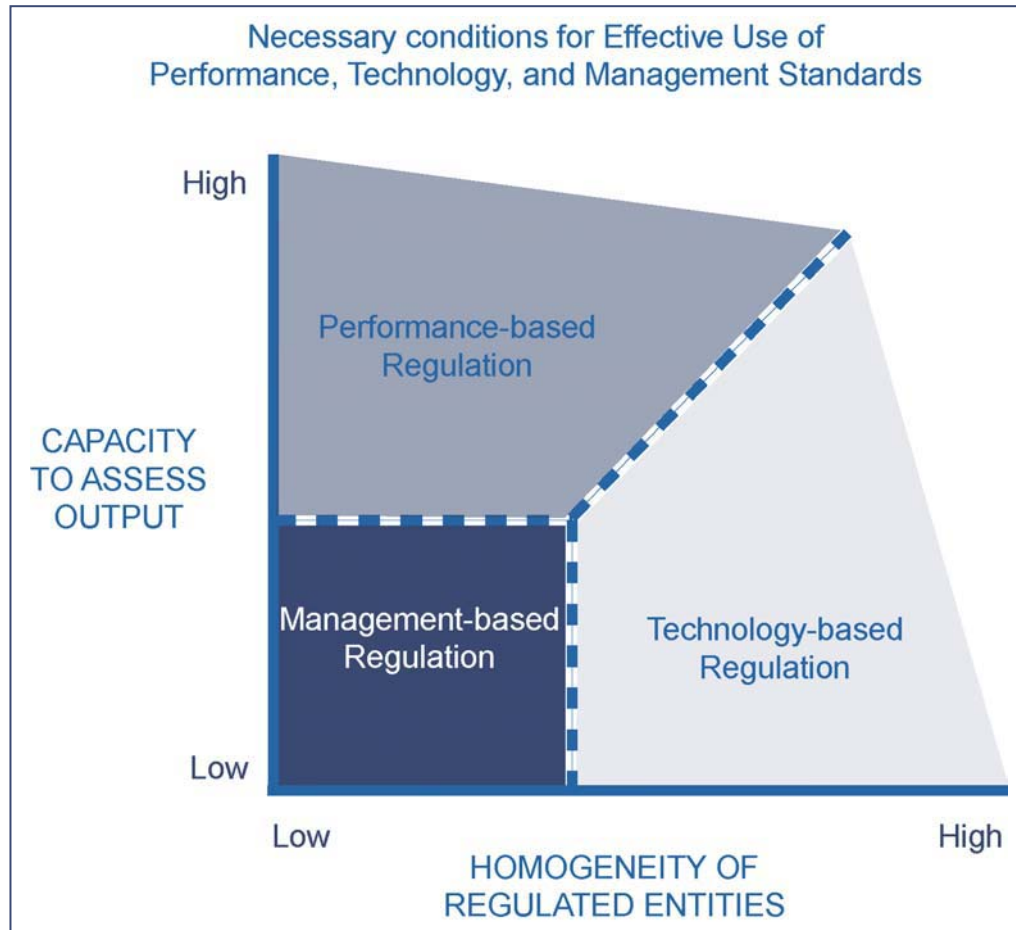


Figure 2: The Structure of Regulation

According to this framework, industries that have highly consistent processes can be regulated by prescribing a set of business procedures that maximize the desired social good (for example, less pollution). But many industries comprise complex processes that vary considerably across companies and over time, making prescription by a regulator difficult and ineffective. In some cases this complexity has led regulators to promulgate performance-based goals for companies. If the processes are distinct but benign, the outcome is easily measured, and the impact is limited when thresholds are only slightly exceeded, then performance-based regulation may be ideal. Minimizing toxic waste at mining sites is one good example.

In many industries, neither process consistency nor continuous output measurement is evident. In cases where the outcome is binary and impact of failure is catastrophic, evidence suggests that management-based regulatory structures are the most effective. The theory is that management will have the most intimate knowledge of its own idiosyncratic processes. When conditions force rapid industry change, management will

be best placed to engineer the most effective process modifications that will achieve the desired social goals.

Nuclear electricity-generating facilities in the United States are a good case in point. Because each was built to a unique blueprint rather than a consistent model, no single set of procedures will guarantee safety across all facilities. And because avoiding a nuclear meltdown is the ultimate regulatory goal, measuring a facility on some continuous dimension of failure is not only meaningless, but the after-effects of such a failure will be catastrophic. In these circumstances, the best regulatory structure might be to establish the social goal (no nuclear meltdown), require that management define its own unique procedures for how it will achieve compliance, provide regulatory evaluation of those procedures, and continuously monitor the facility for internal compliance to the facility's own standards.

Clearly, C-TPAT is a regulatory framework that is leveraging the management-based structure, and this is entirely appropriate. Although significant consistency of process occurs at specific points in supply chains, the consistencies disappear when compliance extends to an end-to-end consideration.

Not surprisingly, when the purview expands to consider extended supply chains, a blended regulatory structure likely will be optimal. Such a blended structure is reflected in C-TPAT Plus, which will rely on consistency in information technology data standards, RFID standards, and standards for evidence of tampering with containers. Part of the regulatory framework will be technology-based.

The Need for Private Sector, Independent Third-Party Verification

Management-based regulation is no panacea, however, Coglianesi and Lazer explicitly describe a set of factors that must be in place to achieve the desired social goals of the regulations. These include setting a floor for the desired specificity of management's plan, deciding how extensively regulators should review management's plans, and establishing standards for record-keeping, monitoring plan implementations, inspections, and third-party auditing.

CBP faces a daunting challenge to organize the many facets of extended supply chains, develop knowledge of best practices, penetrate thousands of companies directly and indirectly involved in supply chains, create awareness and encourage the adoption of best practices that require business process changes, review proposed process changes as management teams adopt varying degrees of commitment to C-TPAT, monitor companies as their supply chain processes evolve, and bring more and more companies into the C-TPAT program. CBP's management-based regulatory structure in C-TPAT is a good fit for the context in which CBP is attempting to achieve its goals. The size and complexity of the task of assuring regulatory compliance mirrors the size and complexity of the US economy.

However, one element of C-TPAT that is not consistent with the management-based regulation is the "inspections and third party auditing." C-TPAT has 7,400 participants

and, so far, a little more than 700 have been validated. CBP acknowledges that validation is not verification.⁹ Coglianese and Lazer state in their study:

Third party audits offer several potential advantages. First, they may create incentives for the inspections themselves to be as efficient as possible. Second, if there are economies of scale in understanding the relevant management systems, third party certifiers specializing in different types of facilities or processes may better capture those scale effects. Lastly, third party auditing can help offset or augment the limited resources of government regulators.¹⁰

CBP's decision to self-police the C-TPAT program is not surprising given scarce Government resources available for compliance verification. How can CBP be expected to verify the security programs of thousands of C-TPAT participants? Moreover, CBP faces severe limitations on its ability to conduct compliance inspections outside the United States at the foreign plants and warehouses where so many supply chains begin. However, will the political leadership and the public have confidence in a self-policing program after a terrorist event, particularly if the event involved a shipment by a C-TPAT participant?

C-TPAT entrusts a vital element of the nation's security to the participants' representations that they are implementing the security policies outlined in the program. In return, the participants receive the benefits of expedited customs processing and potentially a quick restart after an event. Given both the stakes involved and the benefits provided, it is appropriate to create the incentive for private sector, independent third-party auditing to verify those representations. The private sector has mechanisms to do just that, and they should be used.

Enhancing Cargo Security through Private Sector, Independent Third-Party Verification

Private sector, independent third-party verification is a natural enhancement of C-TPAT and any cargo security program. C-TPAT third-party verification would consist of the following:

- Implementation of agreed upon security guidelines
- Agreement on the measures and procedures required to validate the security plans such as effective, efficient, and accurate
- Prescribed intervals for the verification process
- Opinion by an independent auditor that it has tested and verified the security program based upon a set of procedures and testing

⁹ US Customs & Border Protection, "C-TPAT Validation Process Guidelines," http://www.cbp.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/validation_process_guidelines.ctt/validation_process_guidelines.pdf.

¹⁰ *Management-Based Regulation: Prescribing Private Management to Achieve Public Goals*, Regulatory Policy Program, Center for Business and Government, John F. Kennedy School of Government, Harvard University, (2002): 21.

If verified, the participant would meet CBP's requirements for C-TPAT or C-TPAT Plus validation. Management of the participant organization would know that its security program is being properly implemented. Decision-makers could identify and discriminate among supply chains on the basis of security. CBP would have additional data for targeting. If a terrorist event occurs, recovery will require the reopening of the borders and ports. The data from the private sector, independent third-party verification would be available to allow the quick resumption of operations for those supply chains known to be secure. C-TPAT would have fully implemented a true management-based regulatory framework for compliance.

Determining Verification

Verification and the resulting auditor's opinion would be tailored to the specific security program outlined in the agreement between the C-TPAT participant and CBP. The elements of that agreement would reflect the nature of the participant's business and assess the degree of risk that the participant's cargo might be used to facilitate terrorist activity. Verification could be as simple as:

- **Control activities**—Ensure that security policies and procedures are established with a documented series of controls consistent with CBP security guidelines. Controls would be assessed for physical, personnel, and procedural security; access control; manifest procedures; threat awareness; and so forth.
- **Monitoring**—Provide independent testing and verification, including unannounced inspections as appropriate, to ensure compliance that meets the spirit and the letter of the agreed-upon security program. Modifications to the program may also be made as necessary.

Applying Enterprise Risk Management

For programs that are especially complex or for supply chains that pose a greater risk, a more thorough verification could be created by adding other components of a full enterprise risk management regimen.¹¹ These components could include:

- **Internal environment**—Assess the tone of an organization, how risk is viewed and addressed by an entity's people (including risk management philosophy and risk appetite), the organization's integrity and ethical values, and the environment in which the organization operates.
- **Event identification**—Ensure that processes are in place and are effective to identify critical cargo security events. These processes should facilitate prompt response, corrective action, and further risk assessment.
- **Risk profile**—Profile containers using the risk models developed through analysis of the historic marine cargo data and abnormalities in the shipping data. Risk profiling could be further enhanced by correlating existing data on marine cargo shipments and CBP's advance cargo manifest (24-hour rule) data at the time of shipment. This enhanced data could then be used to target containers through CSI.

¹¹ PricewaterhouseCoopers, *Enterprise Risk Management—Integrated Framework*, Committee of Sponsoring Organizations (COSO) of the Treadway Commission, September 29, 2004.

-
- **Risk response**—Management selects risk responses (avoiding, accepting, reducing, or sharing risk), developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.
 - **Information and communication**—Relevant information is identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities. Effective communication occurs broadly, flowing down, across, and up the entity and the supply chain, and extending to the regulator to enable governmental response and action.

Greater Security and Expedited Shipping

The precise scope of the third-party verification and of any required enterprise risk management program could become a standard part of the C-TPAT agreement between the participant and CBP. Such verification and enterprise risk management can and should be applied in any other cargo security program that relies on private sector representations and implementation.

Third-party verification provides the federal government with a commercially proven process to assess and manage risk. This process leverages private sector resources and know-how, creating a level of assurance that may never be obtained through traditional government compliance inspections alone. More importantly, it spreads the cost of that assurance across the broad community that benefits most from continued confidence in the security of the international supply chain—those engaged in international trade.

Although third-party verification will require upfront costs, private companies need only look at the foundation of the shipping industry—speed—to realize the benefit. The economic payback for companies complying with the standards and providing the verification documentation will be the return gained by the speed with which their goods pass through ports of entry. Consistent access to green lanes will be a substantial return to the costs of implementing security standards and having the validation performed.

The success of C-TPAT to date proves that the private sector recognizes these benefits. Raising the bar through the institution of third-party verification should not only lead to further efficiencies in border operations, but it will help protect against a major disruption of supply if a terrorist attack occurs at US ports. Companies failing to comply will face the full impact of delays related to US Coast Guard or CBP inspections.

When a third-party verification system and the application of enterprise risk management tools encompass a partnership of business and government, the result will be greater security. Not only will business and trade benefit, but most importantly, the nation and the American people will as well.

For more information, please contact:

R. Carter Pate, Managing Partner

Tel: 202-414-4400

Email: carter.pate@us.pwc.com

W. McKay Henderson, Partner

Tel: 202-414-1623

Email: w.mckay.henderson@us.pwc.com