

Declaration of inde

Veronique de Rugy argues the case for an independent verification of the US CBP's C-TPAT cargo security programme

According to experts, the United States should be concerned about a nuclear attack by sea. The most plausible scenario is a weapon of mass destruction (WMD) smuggled into the United States in a cargo container. The consequences would be devastating. In addition to the thousands of lives that could be lost, maritime commerce is essential to America's economic vitality. A disruption of that trade would have immediate and significant economic consequences in the United States and also world-wide. The **United States Coast Guard (USCG)** estimates that the closure of even a single major port for one month's time could cost more than \$60 billion in economic losses.

In FY2006, President George W. Bush requested a budget of \$2.03 billion for port security out of a \$50 billion budget for homeland security activities government-wide. However, the important question is not how much money is spent on homeland security, but whether the money is allocated toward the most cost-effective programmes. In other words, is America getting the maximum level of benefit in exchange for its spending?

To be most effective, the money should first go to efforts, such as intelligence programmes, that help prevent devastating terrorist attacks. If experts are correct about the probability of a nuclear attack on the US, then the federal government should make protection of stockpiles of fissile materials a priority. It is also fundamental that spending be directed at keeping nuclear weapons and terrorists out of US ports by implementing security mechanisms to prevent nuclear devices from ever arriving in the United States.

Accordingly, the **Department of Homeland Security (DHS)** has focused some of its efforts on foreign ports. For instance, it is trying to forge relationships with foreign ports to implement container security programmes. The FY2006 budget provides \$138.8 million for this purpose, including \$5.4 million in new funding to expand the Container

'The important question is not how much money is spent on homeland security, but whether the money is allocated toward the most cost-effective programmes'

Security Initiative (CSI), a programme administered by **Customs and Border Protection (CBP)**. The CSI was implemented to target high-risk containers for inspection at overseas ports prior to their departure for US ports (see CBP Commissioner Robert Bonner's article, *Cargo Security International*, December 2004, page 16). To that effect, the CSI deploys teams of inspectors, special agents and intelligence analysts to foreign 'megaports' and other strategic ports to inspect cargo containers cargo for WMDs before they are shipped to the United States. The CSI has put Customs officers in more than 40 overseas ports to monitor containers as they are being loaded (see *Cargo Security International*, December/January, page 8).

The Customs-Trade Partnership Against Terrorism (C-TPAT) is another programme put in place by the DHS and the CBP to improve cargo security while facilitating commerce. C-TPAT will receive \$54.3 million in FY2006. This programme is meant to strengthen the DHS's partnerships with foreign manufacturers and importers. These partners agree to meet supply chain standards for establishing a secure chain of custody for every unit of cargo traded overseas (see *Cargo Security International*, December/January, page 57). The standards ensure that their shipment methods repel potential terrorist attempts to use those shipments for introducing WMDs into US ports. In theory, C-TPAT reduces the need for US port



Veronique de Rugy is a research fellow at the American Enterprise Institute for Public Policy Research (AEI), based in Washington DC, and Board Member and Secretary of the Center for Freedom and Prosperity.

Founded in 1943, the AEI is a private, non-partisan, not-for-profit institution dedicated to research and education on issues of government, politics, economics, and social welfare.

pendence

officials to screen all cargo entering the country and allows them to focus on the most high-risk shipments.

Unfortunately, the DHS has been experiencing difficulties with its foreign programmes. In May 2005, the **US Senate Permanent Subcommittee on Investigations**, led by Senator Norm Coleman, in conjunction with Senators Carl Levin, Susan Collins and Joe Lieberman as well as Representative John Dingell, released two critical **Government Accountability Office (GAO)** reports detailing problems with these two key cargo security programmes. These two GAO reports are the most recent in a series that have found crippling flaws in the CBP's programmes.

The GAO noted that the verification process for applications to the C-TPAT programme does not provide 'an actual verification that the supply chain security measures contained in the member's security profile are accurate and are being followed before the CBP grants the member benefits'. Other weaknesses in the programme, according to the GAO, limit the CBP's ability 'to ensure that the programme supports the prevention of terrorists and terrorist weapons from entering the United States'.

In addition, the GAO reported that 'staffing imbalances' have impeded the ability of CSI ports to target all US-bound shipments. The GAO cited 'political and practical considerations' that have made it difficult for the CBP to develop a model to determine the required level of staff. It appears that the **National Treasury Employees Union (NTEU)** has more to say about where and when Customs inspectors work than homeland security officials do. As a result, 35% of US-bound shipments from CSI ports were not inspected.

The Subcommittee's oversight investigation confirmed these problems and noted that the CBP was not inspecting enough high-risk cargo overseas. In addition, the Subcommittee claimed that the equipment used

'The C-TPAT process of relying solely on supply chain participants to perform self-assessments is not rigorous enough to be effective'

overseas, such as nuclear detection devices and non-intrusive inspection machines, is untested and of unknown reliability. Furthermore, the investigation raised concerns that substantial benefits, including fewer inspections, are provided to certified C-TPAT importers without a thorough validation of their supply chain security; and of those validations that do occur, the process lacks any rigour or independence.

Two recent smuggling incidents demonstrate the inherent vulnerabilities in the global supply chain. On 15 January 2005 and again on 2 April 2005, upwards of 30 Chinese immigrants were found emerging from containers arriving at the Port of Los Angeles. These incidents highlighted security experts' concerns that containers could hold members of terrorist organisations and/or WMDs.

An additional weakness in inspections is highlighted by a new DHS Inspector General report that concludes that there is room for much improvement in the Automated Targeting System (ATS) – the Department's intelligence system to mark high-risk oceangoing containers for further inspections. Approximately nine million oceangoing cargo containers arrive annually at seaports in the US, making it impossible to physically inspect each container without hampering the flow of commerce. Inspectors at overseas CSI ports and at US seaports use ATS to assess the risk associated with each container and determine which containers will undergo inspections.

In theory, through this system, intelligence is used to screen information on 100% of the cargo going to the US. ATS is also a major component of the DHS's efforts to prevent terrorists from sabotaging shipping containers. However, the Inspector General's report questions the completeness and accuracy of the cargo manifests that ATS uses and raises doubts about whether the system is drawing enough shipping data to make accurate risk assessments.

Considering the broad scope of maritime opportunities for terrorists and the dramatic consequences of a successful nuclear or radioactive attack, it is obvious that key elements of the US CBP strategy





are in dire need of repair. A good place to start would be a more systematic implementation of a third-party verification process into CSI and C-TPAT. As the recent study authored by R. Carter Pate and W. McKay Henderson of consultancy firm **PricewaterhouseCoopers (PwC)**, *Cargo Security White Paper: Independent Verification of C-TPAT Cargo Security Controls*, showed, the US 'cargo security plan is only as effective as the system of checks and balances used to ensure it works' (see *Cargo Security International*, December/January, page 7).

As it is now, the C-TPAT process of relying solely on supply chain participants to perform self-assessments is not rigorous enough to be effective. In addition, the government lacks resources to verify security procedures properly and efficiently. As the PwC study noted: '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'.

The report proposed that a private sector, independent third-party verification process be integrated into the C-TPAT and C-TPAT Plus programmes. Potential elements of this process include:

- *Internal environment* – Assess the tone of an organisation, how risk is viewed and addressed by an entity's people (including risk management philosophy and risk appetite), the organisation's integrity and ethical values, and the

environment in which the organisation operates.

- *Event identification* – Ensure that effective processes are in place 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 the 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.

- *Risk response* – Select 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* – Identify, capture and communicate relevant information 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.

There are several important aspects to this approach. First, it would give an active role to the private sector in taking care of

its security instead of relying exclusively on the federal government. It would also give important feedback to the government and create effective checks and balances for the system as a whole. Finally, it structures the incentives to ensure that money is spent on the highest risks and on the most cost-effective programmes. The private sector has always been much better than the government at adopting cost-effective programmes. Also, the independence of a third-party system will guarantee that decisions are made on a sound economic basis rather than politics and bureaucratic process. This would ultimately increase cargo security and the security of the American people.

It seems that nowhere is it more important to develop cost-effective security plans than in the area of maritime security. Rather than investing a massive amount of money in nuclear detection in our ports – where it would ultimately be too late to avoid a catastrophe – a more cost-effective measure is to stop terrorists from bringing WMDs anywhere near our ports. This is achieved by spotting suspicious anomalies while cargos are in foreign ports.

The DHS will be spending roughly \$194 million in FY2006 through its CSI and C-TPAT programmes to secure cargo coming to the US from foreign ports. However, according to experts, the level and depth of this investment is insufficient. To make matters worse, reports also show that these programmes are failing to achieve their basic mission: securing the chain of command. One way to improve these systems would be to encourage public-private partnerships through a third-party verification process that ensures sustainable and effective port security programmes in foreign ports.

Contact:

Veronique de Rugy
American Enterprise Institute
Tel: +1 202 862 7165
Fax: +1 202 862 5807
Email: VDeRugy@aei.org