



September 29, 2006

Highlights of the Conference Report to Accompany H.R. 4954—Security & Accountability For Every (SAFE) Port Act

On September 29, 2006, the conference report, H. Report 109-711, was filed.

Noteworthy

- On September 14, 2006, the Senate voted for final passage of the Senate substitute amendment to H.R. 4954, by a vote of 98-0 (vote No. 249). On September 19, the Leader announced conferees for the bill and negotiation commenced with the House of Representatives.
- On May 4, 2006, the House of Representatives passed H.R. 4954 by a vote of 421–2. The Administration had issued a Statement of Administration Policy (SAP) that generally supported H.R. 4954. On September 12, the Administration issued a SAP on the Senate substitute amendment to H.R. 4954 that was also generally supportive.
- Since the attacks of September 11, 2001 (“9/11”), policymakers have recognized the possibility that our nation’s shipping ports, too, may be terrorist targets. The revelation in August that a major terrorist plot against the United States was in the works by British nationals (who allegedly were planning to exploit security flaws in aviation screening) underscores Congress’s responsibility to address security issues at all of the nation’s portals, including shipping ports.
- Consistent with 9/11 Commission Report recommendations, the Conference Report would require the Department of Homeland Security (DHS) to enhance port security activities by allocating grants *based on risk* to port authorities, facility operators, and State and local government agencies.

Highlights

The Conference Report includes the following:

- **Radiation Monitors at All Ports.** The Conference Report would require that radiation detectors be used on almost all cargo entering the United States at all U.S. ports by December 31, 2008.
- **Identification Cards for Port Workers.** The Conference Report would impose a deadline for the issuance of identification cards for all workers at U.S. ports.
- **Grants.** The Conference Report would change existing law to issue grant funds based on *risk* rather than on principles of *equitable* distribution.
- **Existing Programs.** The Conference Report would authorize and provide guidance on expanding existing programs to screen inbound cargo, and require an expansion of incident planning already required under previous legislation.
- **Non-intrusive Cargo Inspections Systems.** The Conference Report would create pilot programs for integrated non-intrusive cargo inspection systems.
- **New Trade Office.** The Conference Report would create a new office at the Department of Homeland Security (DHS) to enhance international trade.

Background

Port Security: Focus Since 9/11

Since the attacks of September 11, 2001 (“9/11”) using airliners as the means of delivery, policymakers have recognized the possibility that our nation’s shipping ports, too, may be terrorist targets. Currently, some 11 million containers move through U.S. maritime ports on an annual basis.¹ The Administration has adopted a prudent response to such a terrorist threat by utilizing different layers of screening in conjunction with available technology and resources, and upgrading these processes as new technology, resources, and reduced costs make more rigorous inspections feasible.

The Federal government has completed an enormous amount of work to strengthen U.S. ports since 9/11, including passage of the Maritime Transportation Security Act (MTSA) in 2002, and implementation here and abroad of programs governed by U.S. Customs & Border Protection (CBP).

¹ Maritime Containers entering the U.S. totaled 11.3 million in FY2005 (CBP Annual Report). Approximately 60,000 port calls are made each year, constituting 1,258,240,424 metric tons of cargo. U.S. Maritime Administration, “Vessel Calls at U.S. Ports, 2004,” July 2005 (available at http://www.marad.dot.gov/MARAD_statistics/vcalls2004.pdf) and “U.S. Customs Ports 1997-2005” (available at http://www.marad.dot.gov/MARAD_statistics/index.html#Economic%20Analysis).

Advanced Manifest Screening and the Automated Targeting System (ATS)

Under this program, all importers must provide advance manifests of all cargo containers brought into the United States. In this layer of screening, the Department of Homeland Security (DHS) will run computer algorithms using various risk factors associated with the cargo listed in each cargo manifest.² For example, a well-known importer may have its risk score lowered, while an incomplete or inconsistent manifest will be scrutinized more heavily when the cargo reaches the U.S. port. The algorithm computer program, called the Automated Targeting System (ATS), utilizes 240 factors or rules in determining which containers will be considered high risk and targeted for physical and non-intrusive scanning when reaching an American port.³ The intelligence community also contributes information to the targeted inspections system.

Container Security Initiative (CSI)

In an attempt to address these issues, CBP has negotiated agreements with 44 foreign ports, constituting 75 percent of importations to the United States,⁴ to allow for small contingents of CBP agents to inspect cargo as it is loaded onto ships (note that there are over 700, mostly lower-volume, ports importing containers to the United States). This program is called the Container Security Initiative (CSI).

The CBP contingents are too small (due to resource constraints) to inspect all cargo, so they engage in targeted inspections. These officials' ability to target cargo and physically inspect them is dependent upon the good will of their foreign hosts, but cooperative protocols have been worked out to inspect and offload containers. Of great concern to foreign officials is the speed of inspections and their impact on the flow of commerce. Any slowdown costs money for the private traders, domestic commercial interests, and the port itself.

Customs Trade Partnership Against Terrorism (CTPAT)

In an attempt to mitigate some of these problems and make the most efficient use of all its personnel resources, CBP has tried to encourage private importers to beef up the security of their own supply chain. This program is called the Customs Trade Partnership Against Terrorism, or CTPAT.⁵ At present, CBP treats every importer differently, under different standards, depending on local conditions. Very few security plans are physically verified by CBP; however, CBP has

² CBP receives 98 percent of all maritime cargo manifests before they arrive in the U.S. CBP, "Performance and Accountability Report," FY2005, p. 9. The House report for its latest DHS appropriations bill (H.R. 5441) requires that "all inbound cargo is screened through" ATS, p. 9.

³ See Testimony of Richard Stana, Government Accountability Office, House of Representatives Committee on Energy and Commerce, March 31, 2004, GAO-04-557T, and Customs and Border Protection briefing materials for Republican staff, June 23, 2006 (available at RPC upon request).

⁴ Government Accountability Office (GAO), "Container Security: Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts," April 2005, GAO-05-557. Customs and Border Protection briefing materials for Republican staff, June 23, 2006 (available upon request). CBP, "Performance and Accountability Report," FY2005, p. 25.

⁵ CBP, "Securing the Global Supply Chain," available at http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/.

plans to make regular on-site verification of security plans in the near future.⁶ Nevertheless, companies that follow a CBP-approved supply chain security plan obtain a lower risk score when it comes to the container inspections algorithm. In theory, if a company can secure the supply chain, then no terrorist can slip in contraband with that importer's goods in a container bound for the United States. While this is just another layer in the multilayered approach that CBP employs, it is an important step towards enhanced container security.

Non-Intrusive Scanning (VACIS and ICIS)

CBP has employed x-ray scanning, gamma ray scanning,⁷ and radiation detection technologies⁸ in a variety of settings. At U.S. ports, CBP scans 70 percent of arriving containerized sea cargo for radiological material. By the end of FY06, CBP will scan 80 percent of all incoming sea containers for radiation. By the end of 2007, CBP estimates that it will scan 98 percent of all inbound containers for radiation at U.S. ports.

Vehicle and Cargo Inspections System (VACIS) machines are mobile or stationary machines with a large arm employed right at the dock. These machines can be moved over a cargo container, or the container can be placed on trucks as they pass under the VACIS arm. A CBP inspector looks at a video screen, and a black and white image of container content outlines appear. If the manifest describes the container as holding tables, for example, an outline of tables should appear on the screen. If a different image appears, a CBP inspector may mark the container for physical inspection.⁹

One of the weaknesses in the VACIS system is that the image it provides can only reveal so much. For example, tables may appear as one large mass because they are packed with other furniture parts, or tightly packed shoes may not show an outline of shoes. Further, containers passing through such a system must travel at a very slow rate of speed in order for an image to appear. Once the image appears, it can take an inspector up to 15 minutes to evaluate the image; also, there may be considerable problems with scanning fatigue (inspectors cannot remain focused while watching hundreds of images in a given day). Even with the VACIS technology, at the slower rate required for scanning, a massive backlog of cargo would be sitting on the docks. With current technology, consumer costs would mount if 100-percent vetted scanning were required.¹⁰

In Hong Kong Harbor, Science Applications International Corporation (SAIC) (the manufacturer of these non-intrusive scanning devices) is experimenting with three-layered non-intrusive scanning devices. The three layered defense – called the Integrated Cargo Inspection System (ICIS) – is simply the VACIS gamma-ray machine lined together with a radiation portal monitor and an optical character reader used to scan container identification numbers. Incoming

⁶ GAO, "Homeland Security: Key Cargo Security Programs can be Improved," GAO-05-466T.

⁷ Gamma-ray non-intrusive inspection machines can produce images faster than X-ray machines; however, the images have less resolution, especially for densely-packed containers.

⁸ More information on radiation portal monitors is available at www.saic.com/products/security/at-900s.

⁹ According to CBP, "Performance and Accountability Report," FY2005, p. 31, about 8.1 percent of maritime cargo containers were examined using non-intrusive technology such as VACIS.

¹⁰ Fortune 100 estimates that each day a container sits on the docks adds 0.5 percent product value to the cost, Susan Martonosi, et al, "Evaluating the Viability of 100 per cent container inspection at America's Ports," RAND Corp., p. 228, citing C. Spencer, "International Supply Chain Security Regulatory Programs," October 2003.

trucks pass under the monitors at 10 miles per hour while employees monitor the images of the container contents and save copies.¹¹

Currently, ICIS is simply a pilot program that has been funded by SAIC and tolerated by Hong Kong authorities. In fact, the Hong Kong authorities have insisted that ICIS process trucks and containers at no less than 10 miles per hour out of concern that even one lane of slowed traffic due to inspections is enough to seriously hamper commerce. Further, although pictures of container images are taken by employees, CBP has not been able to actually examine the images (although, conceivably, as technology is implemented, images could be sent back to the United States by fiber optic wire to CBP's National Targeting Center for newly developed software to sort and inspectors to examine). These images, too, can only show an inspector so much, and prohibited items can certainly be disguised. From the illegal drug trade, we know, for example, that heroine can be disguised in artwork.¹²

Provisions

The following sections provide a summary of the major sections of the Conference Report.

Title I: General Security for United States Seaports

The Conference Report builds on Maritime Transportation Security Act (MTSA) in requiring incident planning beyond that required under the MTSA. It requires Department of Homeland Security (DHS) to clear waterways, identify salvage equipment, and reestablish the flow of commerce once a maritime transportation security incident occurs. It also authorizes qualified individuals (U.S. citizens or non-watch-listed aliens) to implement DHS-approved security plans for maritime facilities and for DHS to make unannounced inspections of those facilities. DHS would be required to establish a voluntary, long-range, automated vessel tracking system for select vessels, by April 1, 2007. Existing interagency operational/fusion centers would be expanded to all high-priority ports within three years to facilitate coordination and communication among Federal, State, local, and private sector stakeholders.

General Port Operations – Radiation Detection at all Ports

The Conference Report would require DHS to develop and implement, within three years, a national strategy for deployment of radiation detection capabilities. By December 31, 2007, all containers entering the U.S. through its 22 busiest seaports (estimated to constitute 98 percent of all entering cargo) shall be examined for radiation (one year later, the program would be expanded to all remaining ports). DHS must submit a separate plan for the development of equipment to detect weapons of mass destruction (WMD) threats at all U.S. ports of entry. DHS would study the need for port user fees to help fund port security. The Conference Report requires DHS and the State Department to develop a plan for the inspection of passengers and vehicles before

¹¹ SAIC, "Integrated Container Inspection System (ICIS), Hong Kong Demonstration, Frequently Asked Questions," p. 5. Other information in this section was provided by former Customs Assistant Commissioner, John Hensley, presently Vice President SAIC.

¹² Drug Enforcement Agency report on Operation High Step <http://www.dea.gov/pubs/pressrel/pr113005a.html>.

loading onto ferries bound for a U.S. port, within 120 days of enactment. DHS would also have to develop and implement a plan for random physical inspection of shipping containers (DHS already conducts random searches of cargo, but has no formal plan). DHS would also have to establish a rail radiation detection test center, and implant threat assessment screening for trucks entering the country.

Transportation Worker Identification Credential (TWIC)

Under the MTSA, DHS was to create a Transportation Worker Identification Credential (TWIC) for all workers at all U.S. seaports; proposed regulations were published very recently. The Conference Report requires implementation of the TWIC card at the top 10 busiest seaports by July 1, 2007; at the next 40 strategic ports by January 1, 2008; and, at all other ports by January 1, 2009. It also requires DHS to process applications simultaneously for individuals needing both TWIC and merchant mariner documents. TWIC cards cannot be issued to any felon who has been convicted of certain crimes

Grant and Training Programs

Consistent with the 9/11 Commission Report recommendations, the Conference Report would change existing law to require DHS to allocate grants *based on risk* to port authorities, facility operators, and State and local government agencies to enhance port security activities (\$400 million would be authorized for this for FY 07–FY 11). DHS (Coast Guard) would also have to establish a training program for seaport incident management, and create an exercise program to test and evaluate the capabilities of Federal, State, local and other relevant stakeholders to coordinate appropriate response to, and recovery from, threats at commercial seaports.

Title II: Security of the International Supply Chain

DHS would be required to develop and update a strategic plan to improve the security of the international cargo supply chain, including establishing protocols for the resumption of trade; an incident manager would have to implement the plan in reaction to a port security incident. The Coast Guard would (and would be the lead agency to) ensure the safe and secure transit of vessels to U.S. ports. Preference would be given to certain vessels and CSI and CTPAT cargo (see Background section, above) in the resumption of trade.

Cargo Risk Assessment Algorithm: Automated Targeting System (ATS).

As discussed in the Background section above, DHS utilizes advanced submissions of manifest data and the ATS algorithm to provide risk assessment and identify cargo for further inspection. Under the Conference Report, DHS could request the submission of additional data (non-manifest data) for container cargo moving through the international supply chain (authorization of funds is provided). DHS would have to promulgate regulations to establish minimum standards and procedures for securing containers in transit to the United States.

Container Security Initiative (CSI)

The Conference Report would authorize the CSI program (described in the Background section) to identify, examine or search U.S.-bound maritime containers at foreign ports. DHS would establish standards for the use of nonintrusive imaging and radiation detection equipment at CSI ports. DHS would also develop a plan to ensure adequate staffing at CSI ports. (*Note:* although the foreign ports involved in the largest amount of trade with the United States cooperate in the CSI program, most of the over 700 ports importing cargo to the United States do not; staffing has been an issue in the CSI program.)

Customs-Trade Partnership Against Terrorism (CTPAT)

The Conference Report would authorize DHS to establish a voluntary (and already existing) CTPAT program (with minimum standards) to allow importers to cooperate with DHS in securing their own (or their part of the) supply chain. Based on the level of cooperation, security, and verification, CTPAT importers would receive a lower risk assessment score in ATS (and therefore, be less at risk for a full inspection of their cargo and a consequent slowdown in their commercial flow). DHS could deny the benefits in part or in whole, including suspension or elimination for at least five years, of any participant that fails to meet CTPAT requirements or knowingly provides false or misleading information. The CTPAT participants would be broken down into tiers (which DHS would validate and revalidate):

- **Tier 1:** Lower ATS risk score for participants that meet the minimum standards; DHS should complete Tier 1 applications within 90 days of submission.
- **Tier 2:** If these participants meet a higher level of security in their supply chain, they would have reduced cargo examinations and priority processing. DHS would be required to validate the security measures, including on-site assessments, within one year of certification.
- **Tier 3:** If participants meet the highest level of security in their supply chain, benefits would include expedited release of cargo, further reduced examinations, reduced bonding requirements, and notification of specific alerts and post-incident procedures as well as inclusion in joint incident management exercises, as appropriate.

DHS would have to increase, by at least 50 positions annually for FYs 2007 through 2009, the number of personnel to validate and revalidate CTPAT members (authorization of funds is included).

Screening, Scanning, and Integrated Cargo Inspection Systems

The Conference Report would require 100 percent screening to identify high-risk containers (as described in the Background section, the cargo manifests are checked by algorithms). As soon as possible, DHS would have to ensure all containers entering the U.S. undergo integrated cargo inspection scanning, so long as the technology meets certain technical conditions (a report on implementation is due to Congress every 6 months).

The Conference Report would require the development of a pilot program, within one year, in three foreign seaports, each with unique features and varying levels of trade volume, to test integrated scanning systems using nonintrusive inspection and radiation detection equipment (as described in the Background section, above). An evaluation report would be required to be submitted to Congress 120 days after full implementation of the pilot program.

Title III: Administration

Cargo Security Office at Department of Homeland Security

The Conference Report would establish an office within DHS to coordinate all DHS cargo security policy, coordinate DHS cargo security policies with policies of other executive agencies, consult with stakeholders, and establish standards; it also reauthorizes the Homeland Security Science and Technology Advisory Committee to provide outside expertise in advancing cargo security technology.

Research and Development

DHS would coordinate internally and with other public and private sector entities for research and development of maritime and cargo security innovations.

Title IV: Agency Resources and Oversight

Office of International Trade, Cargo Policy and Trade Finance Committees

Customs and Border Protection (CBP) would establish an Office of International Trade, and a Commercial Operations Advisory Committee to oversee implementation of policy for all CBP programs affecting the movement of cargo. DHS would work with appropriate Federal officials and international organizations to harmonize customs procedures, standards, requirements and commitments to facilitate the efficient flow of international trade. Further, the Government Accountability Office (GAO) will conduct a study evaluating the maintenance of the customs revenue function. DHS would work with international organizations to standardize customs procedures and standards.

CBP would complete a resource allocation model by June 2007 and every two years thereafter to determine optimal staffing for commercial and revenue functions; additional CBP personnel to perform commercial operations and customs revenue functions are authorized, along with 1000 CBP officers.

International Trade Data System (ITDS)

The Secretary of the Treasury would be required to oversee the establishment of an electronic trade data interchange system to eliminate redundant information requirements, to efficiently regulate the flow of commerce, and to enforce regulations relating to international trade. All Federal agencies that require documentation for clearing or licensing the importation

and exportation of cargo would have to participate in the ITDS, unless the Office of Management and Budget (OMB) waives the participation requirement based on national security interests.

An Interagency Steering Committee would be created to define the standard set of data elements to be collected, stored, and shared in the ITDS. The Conference Report would require DHS to submit a report to Congress assessing the various aspects of in-bond cargo (tracking, technologies, evaluation criteria for targeting and examining in-bond cargo) and the feasibility of reducing the transit time for in-bond shipments.

Title V – Domestic Nuclear Detection Office

This title authorizes the Domestic Nuclear Detection Office (DNDO, which is already in existence at DHS, but not specified in the Homeland Security Act). The mission of the office would be to develop an enhanced global nuclear detection architecture. The Director of the office would have specific hiring, grant-making, and research authority.

Title VI – Commercial Mobile Service Alerts

The Federal Communications Commission would establish, within 60 days of enactment, an advisory committee to recommend standards to enable a commercial mobile service to make emergency alerts of disasters. The Undersecretary of Homeland Security for Science and Technology would coordinate the development relevant technology research. Grants could be issued to remote locations to be part of the alert system (with a 5-year sunset on grants).

Title VII – Other Matters

This title provides for a Transportation Security Administration (TSA) security plan for essential air service, requires state and local disclosure to DHS of actual expenses under homeland security grants, requires DHS regulations (guided by an Inspector General report 2004-054) relating to trucking security, requires CBP to provide a report on performance indicators relating to the seizure of methamphetamines, and establishes pre-screening for charter flights, among other matters. The title also provides for implementation of a program by the Health & Human Services Department (HHS) whenever a “substance of concern” impacts a disaster area; the program includes alerts to people in impacted areas and requires HHS to provide a report on implementation.

Title VIII – Internet Gambling

This section is fashioned after H.R. 4777, the Internet Gambling Prohibition and Enforcement Act (and H.R. 4411, passed on July 11 by a vote of 317-93, roll call vote no. 363). The bill modernizes the Wire Act of 1961 and expands Title 18 to expand the definition of “wire communication facility” to include Internet or wireless communication facilities.

It redefines "bets and wagers" to include bets for contests, sporting events, games of chance, and lotteries. *Exceptions* include:

- (a) activities governed by securities laws;
- (b) transactions under the Commodity Exchange Act;
- (c) over-the-counter derivative instruments;
- (d) insurance contracts;
- (e) games with only personal efforts at stake; and
- (f) fantasy or simulation sports.

The bill changes the prohibitions against interstate gambling to prohibit the use of the Internet to transmit wagers, and prohibits persons from accepting monies in connection with Internet gambling when those transactions would be illegal in the jurisdiction where the bet was initiated or received. The Internet-based bet would not be illegal if it is made within a single state and it is legal in that state, and it does not violate 15 USC 3001, et seq., 15 U.S.C. 1171, et seq., and 25 U.S.C. 2701 et seq. The Conference Report would also set up civil and criminal penalties for violations of its provisions.

The Department of the Treasury would issue regulations within 270 days designed to block restricted transactions.

The bill also encourages the Executive to gain the cooperation of foreign governments to combat unlawful Internet gambling.