TESTIMONY OF

DEPUTY SECRETARY MICHAEL P. JACKSON

BEFORE THE
SENATE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

April 5, 2006

Chairman Collins, Ranking Member Lieberman, and members of the subcommittee, I am pleased to be here today to discuss S. 2459 – The GreenLane Maritime Cargo Security Act.

Maritime security has been important to the United States since its earliest days. Today we have an efficient maritime transportation system that acts as the backbone of the global economy. That transportation system can also be used to move dangerous cargo to our ports and cities. Any disruptions to that system will have immediate and lasting consequences for our economy and the world at large. The Department of Homeland Security (DHS) commends the work of this Committee in addressing the vulnerabilities of containerized cargo. Our leadership is grateful to this Committee for this hearing and your work to pass important legislation to strengthen maritime cargo security.

Since September 11, 2001 we have made transformational improvements in the extent and quality of the layered system of systems now deployed to strengthen cargo security. This year, the DHS will spend $2.5 billion on maritime security. Overall, the Federal Government is spending $2.8 billion, including the Department of Energy's Megaports program. If the President's FY 07 budget is enacted, we will have spent some $9.6 billion in this area in four years (FY04-FY07).

Today I would like to talk particularly about the path ahead to strengthen maritime cargo security from a risk perspective. We have focused above all on the Weapons of Mass Destruction (WMD) threat because of its potential impacts, but I will also touch on measures that will strengthen our ability to detect all forms of contraband and address other risks.

A Layered System of Systems Supporting a Global Network. First, a brief word about our overall approach to maritime cargo security. Our security doctrine is grounded on a commitment to deploy a strong, layered system of security systems. By deploying multiple, mutually reinforcing security layers and tools, we diminish the risk associated with failure at a single point. Some layers may have a more immediate and obvious security function, such as the physical inspection of a container by Customs and Border Protection (CBP) field agents. Others, such as the Administration's work in global nuclear non-proliferation are complementary, aimed at making it more difficult to acquire WMD components. Security is seldom adequately delivered via a single silver bullet.

It begs the obvious, but bears noting, that we are talking about a *global supply chain* that serves an *interdependent global economy*. Thus, a second doctrinal component of our cargo security strategy has been, where possible, to push security measures out beyond our borders. Close partnerships with the private sector are essential because the private sector owns most of the assets and moves the goods. CBP's Customs-Trade Partnership Against Terrorism (C-TPAT) is an example of such a partnership program.

It strengthens our hand to partner closely with other governments, which is why bilateral and multilateral solutions to supply chain security continue to be a focus for this Administration. The Container Security Initiative (CSI) and our work with the World Customs Organization, the International Maritime Organization and the International Standards Organization have improved security.

Existing Security Architecture. The existing security architecture consists of four core components: (1) vessel security; (2) personnel security; (3) cargo security; and (4) port facility security. Some elements of each of these four components are focused abroad, others at home – thus there are essentially eight areas of activity that capture most of the programmatic focus of our supply chain security work. The draft legislation that is the focus of this hearing appropriately seeks to strengthen most of these categories.

I would like to discuss two particular areas that present significant near-term upside for improving security: (1) improvements regarding DHS's targeting of highest-risk containers and our tools used to inspect containers; and (2) deployment of the Transportation Worker Identification Card for unescorted access to U. S. ports.

Secure Freight. The Department's Secure Freight initiative has two major components: better targeting and enhanced inspection tools.

Better Targeting. CBP's Automated Targeting System (ATS), which is used by the National Targeting Center and field targeting units in the United States and overseas, profiles inbound cargo and identifies high-risk cargo entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags," and determine which passengers and cargo are high risk, and therefore should be scrutinized overseas or at the port of entry.

ATS is a flexible, constantly evolving system that integrates enforcement and commercial databases. ATS analyzes electronic data related to individual shipments prior to arrival and ranks them in order of risk based on the application of algorithms and rules. The container scores are divided into thresholds associated with further action by CBP, such as document review and inspection.

ATS is an extraordinarily powerful "first generation" tool, and a more sophisticated, next-generation tool is under development at DHS as part of the Secure Freight initiative. ATS data is derived from filings of cargo waybills and an extensive historical risk scoring algorithm derived from years of data about containers and inspections.

The next-generation tool will fuse existing data along the supply chain gathered from multiple actors who touch the box from the order, to container origin, to destination. This data aggregation would, in my view, best be fused by a third party intermediary – perhaps formed by the industry itself. The U.S. government would then receive this richer set of data about each container move in advance of lading overseas. It would then inform CBP's container risk assessments. Ideally, the U.S. government would certify one or more such qualified entities formed for this purpose, and would set standards for such data fusion. The intermediary would be rigorously audited.

This approach is the natural extension of the requirement to have better data upon which to score risk of inbound containers. It would support not only the needs of the United States better to understand and assess risk of inbound containers, but also could serve the exact same needs for other nations. This would serve to improve security in the global cargo network and in more nations. This next-generation tool will not grow overnight. But stronger container profiling is possible, and I am convinced that we can make great progress in the near term. I ask this Committee to support our efforts in this area, and would welcome an opportunity to elaborate further in response to your questions.

Enhanced Inspection Tools. Better detection systems can be deployed both abroad and at home. At home, our goal is to have 100 percent inspection of all containers that are transported by truck or rail from a U.S. port into the interior of our country. Abroad, our goal is to increase materially the number of containers inspected by radiation detection tools and by non-intrusive inspections, including large-scale X-ray devices. The Domestic Nuclear Detection Office (DNDO) recently tested new and better fixed, mobile and handheld radiation detection equipment that can be deployed to ports of departure, ports of entry and the marine environment.

In this regard, I would note that last week Secretary Chertoff was in Hong Kong and saw first-hand the Integrated Container Inspection System (ICIS) pilot program underway there. CBP is engaged in a technical exchange to evaluate how the data gathered by ICIS can be used to strengthen our inspection capabilities. After extensive discussion with industry about the ICIS pilot and its underlying technology and business concepts, I am highly optimistic that this pilot can point the way to a collaborative network that can significantly enhance CBP's capabilities physically to inspect a larger number of containers from points worldwide. I'd be happy to discuss with the Committee DHS's thought about how this might develop.

Transportation Worker Identity Card (TWIC). On Friday of last week, the Transportation Security Administration (TSA) published a "request for qualifications" seeking firms who are appropriately experienced and interested to help DHS deploy certain components of the TWIC program. The TWIC architecture, compliant with FIPS-201 technical architecture, will provide an open standard and ensure interoperability and real-time exchange for supply chain security cooperation between the Department and the private sector. This is the first step toward operational deployment of the TWIC program for unescorted access to all U.S. ports. This day has been too long in coming.

This deployment includes accelerated and parallel rulemakings by both TSA and Coast Guard. And it includes a procurement needed to help launch the operational program. Secretary Chertoff has given his team instructions to get this done as quickly as possible. Further details will be forthcoming as part of the rulemaking and procurement actions. This tool will add another valuable layer of security to domestic port operations and will strengthen overall supply chain security.

S. 2459 – The GreenLane Maritime Cargo Security Act. The Department is committed to moving forward on all eight areas of activity regarding cargo security. We believe that this proposed legislation reflects a great deal of solid agreement with DHS, and we will continue to work with the Committee as you continue to work on this legislation. At this point I would like to offer comments on a few specific sections of the GreenLane Maritime Cargo Security Act.

Next Generation ATS. Your legislation calls for improvements in CBP's ATS capability. As my previous discussion of the Department's Secure Freight Initiative shows, we agree that this already powerful tool should be made stronger. We very much look forward to working with Congress on operational details of a second-generation system.

The Movement of Radiological Material. The capacity to detect and identify the illicit movement of radioactive materials across our borders in the commercial supply chain is a critical concern of the Administration. DNDO is working closely with CBP to develop a new deployment strategy that will provide an optimized mix of current and next-generation systems to balance capability, coverage and cost. That deployment strategy will result in screening 98 percent of all containerized cargo crossing the southern border by fiscal year 2006 and at seaports by fiscal year 2007.

The GreenLane Concept. DHS agrees with the concept that we should provide incentives to encourage adoption of security practices that go beyond those mandated by law and regulation, such as practices already adopted by third-tier C-TPAT members. Indeed, vessels that carry cargo that have followed more rigorous security practices throughout the supply chain will tend to be lower risk. This fact should help us triage risk following a maritime incident to resume the flow of commerce.

However, the ability for the DHS to maintain flexibility in allocating benefits and responding to changes in threat is key. As a minimum, a GreenLane program should consider several factors, especially in reestablishing the flow of commerce following an incident. The first factor is the specific nature of the incident. If the incident involved attacks by small boats or other factors not related to the security of the vessel and its cargo, recovery operations would focus less on threats presented by the supply chain. Tactical intelligence could also form a basis for considering certain vessels higher-risk, but the ability to require all containers on a vessel to be GreenLane eligible is not logistically feasible at this point in time. National priorities connected to public health and safety, or support for military logistics, are other factors that should influence the decision on reestablishing the flow of commerce following an incident. The infrastructure of the port along with the ownership and operation of specific terminals also must be considered.

Under Secretary for Policy. We strongly agree with the Committee's proposal to establish an Under Secretary for Policy in the Department as called for in our 2SR recommendation. The legislation also calls for the establishment of a Director of Cargo Security Policy, who will report to the Under Secretary of Policy, to coordinate Department-wide cargo security policies and programs with other executive agencies relating to cargo security. We are moving ahead to implement this recommendation by actively recruiting a well-qualified individual to lead this effort.

Port Security Grants. While the legislation does not specify whether the port security grant program authorized is part of the Administration's proposed Targeted Infrastructure Protection Program (TIPP), I would like to take this opportunity to reiterate that the Administration supports the creation of the TIPP to enable increased funding for protecting infrastructure on the basis of risk that may, if warranted, increase funding for ports. Under the President's FY07 budget request, $600 million is requested for the TIPP grants, which would allow additional resources to flow to port security needs based upon the most up-to-date threat risk assessment.

Technology Investments. The DHS fully supports the concept of investing in research and development to improve our maritime cargo security. The DHS is engaged in a substantial amount of research and development on maritime cargo security solutions, which includes bringing to bear the innovation and market forces of the private sector. While we differ in our method and timing on container standards, we agree in the need to launch a six-sided container intrusion detection system. The DHS is participating in a number of development efforts regarding container standards. We must ensure that any standards are based on the right technology, lest the rush to endorse a standard could result in operational practices that do not appreciably enhance security and may unintentionally impede international trade.

Conclusion. The Department is working closely with other government departments and agencies, with industry, and the international community to establish workable solutions to improve supply chain security. We recognize the challenges that face our programs and the importance of protecting our nation from terrorist threats to our vital economic engine. We are making significant progress. I would like to thank the Senate Committee on Homeland Security and Government Affairs again for this opportunity to discuss our efforts and comment on this legislation which is so important to the Department and the nation.

This completes my prepared statement. I would be happy to answer to any questions you may have.