TESTIMONY OF

DEPUTY SECRETARY MICHAEL P. JACKSON

BEFORE THE
SENATE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

UNITED STATES SENATE

MARCH 30, 2006

Chairman Coleman, Ranking Member Levin, and members of the subcommittee, I am pleased to be here today to discuss the critically important issue of global supply chain security.

Secretary Chertoff has repeatedly spoken about the importance of using risk-based assessments to focus our efforts on threats that present the greatest consequences. It is not possible to eliminate all risk, but we must focus on the highest risks with tenacity and creativity. Clearly, defending against the use by terrorists of weapons of mass destruction (WMD), particularly radiological and nuclear devices, is the highest priority of our maritime cargo security efforts.

Mr. Chairman, this subcommittee and the full Committee have been consistently focused on these issues, and committed to innovation. I want to assure you that the Department of Homeland Security (DHS) shares your commitment to strengthen supply chain security. I am personally committed to nurturing a healthy dose of urgency within DHS to deliver continuous improvement in this area. We can afford no less.

Since September 11, 2001 we have, however, 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 some $2.5 billion on maritime security. Overall, the Federal Government is spending $2.9 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). Earlier this week, colleagues from Customs and Border Protection (CBP), DHS' Domestic Nuclear Detection Office, and the Department of Energy testified to you about this work and the tools we have already put in place. So I'll try not to duplicate the detailed testimony they provided.

We could not have come this far without the full engagement and serious commitment of thousands of private sector partners around the globe. Representatives of several organizations and businesses participating closely in this work will testify later today. DHS is grateful for their shared commitment to secure the supply chain.

Although we have made great progress, more needs to be done. In fact, we must be institutionally disciplined to understand that our commitment to stay ahead of those who would do harm to our people and our economy can never cease. Terrorists will continue to probe our systems and will themselves innovate. Still a young organization, DHS must operate every day with urgency and discipline, while casting our eyes to the future.

Today I'd like to talk particularly about the path ahead to strengthen security for the global supply chain. I will focus on the WMD threat because of its centrality, but will also touch on measures that will also strengthen our ability to detect all forms of contraband. Secretary Chertoff has launched the Secure Freight initiative to implement aspects of the work ahead for DHS and the industry.

A Layered System of Systems Supporting a Global Network. First, a brief word about our overall approach to supply chain security. Our security doctrine is grounded upon 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 CBP field agents. Others, such as the Administration's work in global nuclear non-proliferation are complimentary, aimed at making it more difficult to acquire WMD components. Security is very 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. It has required close partnerships with the private sector, because they own most of the assets and move the goods. As the recent debate about the now abandoned DP World transaction within the United States underscores, the basic facts about who owns and operates the global supply chain can cause concerns.

With whom should we partner and how? A fair question. But there is no question that we must partner to ensure both security *and* mobility. CBP's Customs-Trade Partnership Against Terrorism (C-TPAT) is an example of such a partnership program. Here, the aphorism made famous by President Reagan guides: trust but verify. C-TPAT's verification regime is an example of our doing that.

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

Some of the first generation layers of security will give way to second-generation tools. Others will be strengthened. New tools will be added. Not all of the layers are

appropriately unpacked in public hearings. But perhaps it would be useful simply to lay out the basic structures for supply chain security and elaborate on those areas that I consider most ripe for accelerated improvement.

Existing Security Architecture. An outline of the existing security architecture includes 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 buckets of activity that capture most of the programmatic focus of the supply chain security challenge.

Most of the core federal programs were explained in detail by DHS testimony earlier this week. I'd just supplement that testimony with a quick overview of the Coast Guard's role in securing the supply chain at home and abroad. Their implementation of the Maritime Transportation Security Act (MTSA) in the United States and the International Ship and Port Facility Security (ISPS) Code abroad forms the basis for securing the foreign and domestic ports and vessels that are the foundation of the international marine transportation system.

At home, the Coast Guard routinely inspects and assesses the security of 3,200 regulated facilities in more than 360 U.S. ports at least annually in accordance with MTSA and the Ports and Waterways Security Act. Every regulated U.S. port facility, regardless of owner/operator, is required to establish and implement a comprehensive Facility Security Plan that outlines procedures for controlling access to the facility, verifying credentials of port workers, inspecting cargo for tampering, designating security responsibilities, training, and reporting of all breaches of security or suspicious activity, among other security measures. Working closely with local port authorities and law enforcement agencies, the Coast Guard regularly reviews, approves, assesses and inspects these plans and facilities to ensure compliance.

In accordance with MTSA, the Coast Guard has completed verification of security plans for U.S. port and facilities and vessels operating in U.S. waters. Specifically,

- Port Threat Assessments for all 55 militarily or economically critical ports have been completed. The Coast Guard has developed 44 Area Maritime Security Plans covering 361 ports, the Great Lakes, the Inland and Western Rivers and the Outer Continental Shelf region.
- The Coast Guard completed initial security plan verification exams on all 6,200 U.S. flag inspected vessels on July 1, 2005.
- The Coast Guard has completed 2,400 verification examinations on un-inspected vessels regulated under the MTSA, and is on track to complete all 4,800 by December 31, 2006.

In addition, the Automatic Identification System has been fielded at 9 ports with Vessel Traffic Service systems and allows the Coast Guard to identify and track vessels in the coastal environment. Long range tracking, currently in development, will enable the

Coast Guard to identify and track vessels thousands of miles at sea, well before they reach our coastal zones. Likewise, the Inland River Vessel Movement Center provides critical information about the movement of hazardous cargoes along our nation's inland rivers.

The Coast Guard has also established 12 Maritime Safety and Security Teams and enforced hundreds of fixed and moving security zones to protect Maritime Critical Infrastructure and key assets and naval vessel protection zones to protect U.S. Navy and Maritime Administration vessels. Further, the Coast Guard is developing a risk-based decision making system, to be implemented this year, which will help prioritize high capacity passenger vessels escorts. Although initially developed for high capacity ferries, its application is being expanded to enhance current security measures for other high capacity vessels: ferries, cruise ships, and excursion vessels carrying 500 or more passengers.

Abroad, the Coast Guard conducts foreign port security assessments through its International Port Security Program. To date the Coast Guard has assessed 45 countries, with 40 having been found to be in substantial compliance with the International Ship and Port Facility Security Code. These 45 countries are responsible for over 80 percent of vessel arrivals to the United States. The five countries that are not in substantial compliance have been notified to take corrective actions or risk being placed on a port security advisory and have conditions of entry imposed on vessels arriving from their ports. The Coast Guard is on track to assess approximately 36 countries per year with an ultimate goal of visiting all of our maritime trading partners within four years.

Finally, in addition to the work of the Coast Guard, the Port Security Grant program (PSGP) has awarded over $700 million to owners and operators of ports, terminals, and U.S. inspected passenger vessels and ferries, as well as port authorities and State and local agencies to improve security for operators and passengers through physical security enhancements. These grants are intended to create a sustainable, risk-based effort for the protection of ports from terrorism, especially explosives and non-conventional threats that would cause significant loss of life and major disruption to commerce.

As part of the FY 2005 PSGP, significant changes were introduced to make the program more risk based. And it required certain grantees to supply matching funds, which added some $30 million more to this program. Changes include limiting eligibility to the nation's most at-risk seaports and distributing funding based on risk, needs and national priorities for port security.

I'd like now to focus on two particular areas that present significant upside for improving security: (1) improvements regarding DHS's targeting of containers of highest risk and tools 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 at the port of entry or overseas.

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 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 the cargo waybill and an extensive historical risk scoring algorithm derived from years of data about containers and inspections.

The next-generation tool will fuse existing data from across the supply chain by multiple actors who touch the box from order, container origin, to destination. The 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 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 of other nations. This is not a tool that will grow overnight. But stronger profiling is possible, and I am convinced that we can make great progress in the near term. I would welcome an opportunity to elaborate further in response to questions.

Enhanced Inspection Tools. My DHS colleagues testified already about DHS's plan to expand rapidly the number and the performance of radiation portal monitors and the next generation tool, Advanced Spectroscopic Portals. The Domestic Nuclear Detection Office has recently tested new and better handheld radiation detection equipment, which we will deploy in the marine environment.

Better detection systems can be deployed both abroad and at home. At home, our goal is to have 100 percent inspection of all containers as they depart a U.S. port headed into 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.

In this regard, I'd note that this week Secretary Chertoff will be in Hong Kong to see first-hand the Integrated Container Inspection System (ICIS) pilot 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. I understand that several members of this subcommittee have had the opportunity to inspect the same pilot program.

After extensive discussion with industry about the ICIS pilot and its underlying technology and business concepts, I find myself 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. Again, I'd be happy to discuss with the subcommittee DHS's thought about how this might develop.

Transportation Worker Identity Card (TWIC). On Friday of this week, the Transportation Security Administration (TSA) will publish a "request for qualifications" seeking firms who are appropriately experienced and interested to help deploy certain components of the TWIC program. 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 will include accelerated and parallel rulemaking work by both TSA and Coast Guard. And it will include 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 a valuable layer of further security to domestic port operations and will strengthen overall supply chain security.

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 this vital economic engine. We are making significant progress. The Department thanks you for your continued support and looks forward to working with you as these programs further develop and mature.

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