

---

**STATEMENT OF RICHARD L. SKINNER**

**ACTING INSPECTOR GENERAL**

**U.S. DEPARTMENT OF HOMELAND SECURITY**

**BEFORE THE**

**COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION**

**UNITED STATES SENATE**

**MAY 17, 2005**



Mr. Co-Chairman and Members of the Committee:

Thank you for the opportunity to be here today to discuss the work of the Office of Inspector General (OIG) regarding port and maritime security. I would like to address three areas related to security: preventing terrorist weapons from entering the United States, maritime security challenges facing the U.S. Coast Guard (USCG), and the Port Security Grant Program. These areas involve major components of the Department of Homeland Security (DHS) and its wide-ranging operations. Each has been the subject of oversight by the OIG and my comments are drawn from our reports, which are available on the OIG website at [www.dhs.gov/oig](http://www.dhs.gov/oig).

### **Preventing Terrorist Weapons from Entering the United States**

Since September 11, 2001, the Department of Homeland Security's Bureau of Customs and Border Protection's (CBP) priority mission is detecting and preventing terrorists and terrorist weapons from entering the United States. A major component of its priority mission is to ensure that oceangoing cargo containers arriving at the seaports of entry are not used to smuggle illegal and dangerous contraband. To test controls over importing weapons of mass destruction, ABC News was successful in two attempts at smuggling depleted uranium into the country. On September 11, 2002, ABC News reported that a 15-pound cylinder of depleted uranium was shipped from Europe to the U.S. undetected by CBP. On September 11, 2003, ABC News reported that the same cylinder was smuggled to the U.S. from Jakarta, Indonesia, again undetected.

In the first smuggling event, ABC News reported that a steel pipe containing a 15-pound cylinder of depleted uranium, which was shielded with lead, was placed in a suitcase and accompanied by ABC News reporters by rail from Austria to Turkey. In Istanbul, Turkey, the suitcase was placed inside an ornamental chest that was crated and nailed shut. The crate containing the suitcase was then placed alongside crates of huge vases and Turkish horse carts in a large metal shipping container, and then loaded onto a ship that left Istanbul. Based on data contained in the Automated Targeting System, the crate was targeted as high-risk for screening by the U.S. Customs Service (Customs). ABC News broadcast on September 11, 2002, that Customs failed to detect the depleted uranium carried from Europe to the United States.

During the second smuggling event, ABC News placed the same cylinder of depleted uranium into a suitcase, and then placed the suitcase into a teak trunk. The trunk, along with other furniture, was loaded into a container in Jakarta, Indonesia, and then transshipped to the U.S. from Tanjung Pelepas, Malaysia. This shipment was also targeted as high-risk for screening and subsequently inspected by CBP personnel, but was then allowed to proceed from the port by truck.

In a classified September 2004 report, *Effectiveness of Customs and Border Protection's Procedures to Detect Uranium in Two Smuggling Incidents*, we cited several weaknesses that occurred at the time of the two incidents that made the container inspection process ineffective. The protocols and procedures that CBP personnel followed at the time of the

two smuggling incidents were not adequate to detect the depleted uranium. CBP has since enhanced its ability to screen targeted containers for radioactive emissions by deploying more sensitive technology at its seaports, revising protocols and procedures, and improving training of CBP personnel.

At the request of four congressional committees, we recently initiated a follow-up audit to determine the status of CBP's implementation of the recommendations made in our September 2004 report. In addition, we will review other relevant technologies and implementation plans recommended by entities associated with CBP's efforts to increase the detection capability of the radiation portal monitors that are deployed domestically and internationally.

### **Maritime Security**

The Coast Guard's willingness to work hard and long hours, use innovative tactics, and work through partnerships in close inter-agency cooperation has allowed it to achieve mission performance results goals. However, to improve and sustain its mission performance in the future, the Coast Guard faces significant barriers, most importantly the deteriorating readiness of its fleet assets. The Coast Guard faces three major barriers to improving and sustaining its readiness to perform its legacy missions:

1. The lack of a comprehensive and fully defined performance management system impedes the Coast Guard's ability to gauge its performance, allocate resources effectively, and target areas for improved performance.
2. The workload demands on the Coast Guard will continue to increase as it implements the Maritime Transportation Security Act of 2002 (MTSA). This complex work requires experienced and trained personnel; however, the Coast Guard has in recent years suffered from declining experience levels among its personnel.
3. Sustaining a high operating tempo due to growing homeland security demands, such as added port, waterway, and coastal security patrols, will tax the Coast Guard's infrastructure including its aging cutter and aircraft fleet.

The lack of a comprehensive and fully defined performance management system impedes the Coast Guard's ability to gauge its performance, allocate resources effectively, and target areas for improved performance. The Coast Guard has yet to define a performance management system that includes all the input, output, and outcomes needed to gauge results and target performance improvements, balance its missions, and ensure the capacity and readiness to respond to future crises or major terrorist attacks. For example, for search and rescue, the number of mariners in distress saved is a good indicator of outcome; however, resource hours under-represent the effort put into this mission by omitting the many hours of watch standing at stations. Without more complete information, the Coast Guard has limited ability to identify and target cost effective improvements to mission performance.

The workload demands on the Coast Guard will continue to increase as it implements the MSTA. Under MTSA, the Coast Guard must conduct risk assessments of all vessels and facilities on or near the water; develop national and area maritime transportation security plans; and approve port, facility, and vessel security plans. This complex work requires experienced and trained personnel, presenting a major challenge for the Coast Guard, which has in recent years suffered from declining experience levels among its personnel. Since the Coast Guard largely relies on experienced senior personnel to coach and train junior personnel and new recruits on the job, mission performance is at risk.

In addition to implementing MTSA, growing homeland security demands, such as added port, waterway, and coastal security patrols, result in a continued high operating tempo. Sustaining this high operating tempo will be a major challenge for Coast Guard personnel and will tax its infrastructure, especially its aged cutter and aircraft fleet. The Coast Guard reported that mission sustainment is at risk due to cutters and aircraft that are aging, technologically obsolete, and require replacement and modernization. Currently, the Coast Guard is experiencing serious cracking in the hulls of the 110 foot cutters and engine power loss on the HH-65 Dolphin helicopters, resulting in operating restrictions. These problems adversely affect the Coast Guard's mission readiness and ultimately mission performance.

### **The Port Security Grant Program**

The department's Port Security Grant Program is designed to reduce the vulnerability of American ports to potential terrorist attacks by enhancing facility and operational security. The Transportation Security Administration, the U.S. Coast Guard, and the Department of Transportation's Maritime Administration have collaborated to award over \$560 million for over 1,200 projects. My office reviewed the design and goals of the program, the roles and responsibilities of participating agencies, and the grant evaluation and selection process. The bulk of our analysis focused on grant award decisions in rounds two and three. The results of our review are discussed in our January 28, 2005 final report, *Review of the Port Security Grant Program (#OIG-05-10)*. We identified several important issues relating to the strategic direction of the program, the program's support of national infrastructure protection priorities, and the general administration of the program. I would like to briefly talk about those results.

First, the program's strategic effectiveness is hindered mainly because it is attempting to reconcile three competing approaches: the competitive program mandated by Congress, MTSA's grant authority, and risk-based decision making. These competing approaches are clouding the direction of the program. The program is under pressure to help defray the costs of the MTSA security mandates that broadly affect the maritime industry. MTSA included a grant authority intended to equitably distribute funds for this purpose, but the appropriations legislation did not fund the MTSA port security grant program and required a competitive grant program focused on securing national critical seaports. However, the resulting program must base award decisions on the universe of applications submitted – which may or may not include the most critical needs. In addition, the evaluation and selection process emphasized awarding funds to as many

applicants as possible. Hence, the program attempted to balance the competitive program that objectively evaluates the quality of the applications with the need to broadly disperse funds to assist with MTSA compliance, while at the same time incorporating risk-based eligibility criteria and evaluation tools to prioritize projects.

Second, the program did not have the benefit of national key asset and critical infrastructure protection information now being developed by the Information Analysis and Infrastructure Protection (IAIP) directorate. Program administrators and IAIP, which is responsible for developing strategies for protecting the nation's critical infrastructure, did not collaborate to integrate the program with broader national security initiatives. Thus, port security grant award decisions were made without sufficient information about our national priorities.

Third, grant award decisions were made with the intent of expending all available funding and spreading funds to as many applicants as possible. The program funded projects despite dubious scores by its evaluators against key criteria, raising questions about the merits of 258 projects costing \$67 million. It appeared that headquarters and field reviewers did not share a common understanding of program objectives or eligibility criteria. Frequently, they did not agree about the eligibility or merit of projects and did not consistently document their rationale for recommending or not recommending funding. We pointed out the need for the program to look more closely at the first three criteria (whether the grant proposal was in an area of high risk, addressed a critical security need/vulnerability, and provided high risk reduction), which were well conceived and should have carried more weight.

In addition, the program forwarded an additional 82 projects to the Office of Domestic Preparedness to be funded at a cost of \$75 million under the Urban Area Security Initiative, despite previously determining that these projects did not merit funding.

Another dilemma for the program is the question of where the private sector's responsibility for preventing terrorism ends and where the federal government's responsibility begins. At the time of our report, DHS did not have a formal policy to provide financial assistance to private entities, a group that includes those that own and operate high risk facilities. Even though private entities have applied for and received substantial funding, we did not conclude that the program should limit funding to the private sector per se. However, some of the grants to private companies were within the financial reach of the applicants and many were for basic security measures that should have been considered normal costs of doing business. For example, some of the projects were for anti-theft purposes and not related to terrorist attack prevention or deterrence.

Furthermore, after three rounds, recipients spent only a small portion of the entire amount awarded. Of the \$515 million awarded between June 2002 and December 2003, including \$75 million provided under the Office for Domestic Preparedness' Urban Area Security Initiative, grant recipients had expended only \$106.9 million, or 21 percent of total program awards as of September 30, 2004. As a result, the majority of projects had not

been completed and the program had not yet achieved its intended results in the form of actual improvements to port security.

This brings us to the status of our recommendations. In response to our draft report, DHS concurred with 11 of our 12 recommendations. In our final report, we strongly encouraged DHS to fully implement our recommendations before proceeding with the next round of port security grants. DHS' Office of State and Local Government Coordination and Preparedness (SLGCP) received \$150 million in the FY 2005 budget for round five of the port security grant program. SLGCP officials informed us that they were going to make substantive changes to the design of the program to make it more risk-based, and while it appears they have, we have not evaluated the effect of these changes.

We recently received DHS' action plan, which discusses corrective actions taken and planned in response to our recommendations. The action plan generally appears to be responsive to our recommendations. For example:

- We identified numerous projects within ports not on the list of strategic or controlled ports. The program developed and implemented a funding distribution model that targeted 66 ports as eligible under the program.
- We noted the lack of a policy for funding private sector projects. The action plan refers to a decision by the Secretary that private entities may apply for a grant, but must provide matching funds of 50 percent.
- Program administrators did not collaborate with IAIP on broader national security initiatives. SLGCP is taking steps to improve information sharing with, and participation of, IAIP in the selection and evaluation process.

However, we are also reviewing additional information supporting the action plan. In addition, we have not had the opportunity to review guidance that will be issued for those SLGCP, USCG, TSA, CBP, IAIP, and MARAD personnel who will be evaluating projects. The revised grant application package was just released this past week. We are studying how DHS has modified the program--particularly the criteria program administrators will use and how they will apply it during the evaluation process--and whether those modifications satisfy our recommendations. We expect to communicate this information to SLGCP in the near future.

Mr. Co-Chairman, this concludes my prepared statement. I will be pleased to answer any questions you or the members may have.

# # #