

DEPARTMENT OF HOMELAND SECURITY
Office of Inspector General

Follow Up Review
of the
Port Security Grant Program



Office of Inspections and Special Reviews

OIG-06-24

February 2006
(REVISED)



**Homeland
Security**

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibility to promote economy, effectiveness, and efficiency within the department.

This report assesses the actions DHS has taken to strengthen the administration and effectiveness of the port security grant program since our previous report on the program. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations have been developed to the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General

Contents

Executive Summary	1
Background.....	2
Results of Review	4
The Port Security Grant Program is More Strategic (Prior Report Recommendation Nos. 1, 12)	4
The Office of Infrastructure Protection Fills Necessary Role (Prior Report Recommendation No. 2).....	6
Improved Evaluation and Selection Process Reduces, but does not Eliminate, Concerns about Funding Unworthy Projects (Prior Report Recommendation Nos. 3 – 5)	6
Field Reviewers Scored Projects Differently (Prior Report Recommendation Nos. 6 – 8)	14
Private Sector Policy Should Address Prudence of Funding Certain Projects (Prior Report Recommendation No. 9).....	16
Balance of Unspent Funds is Declining (Prior Report Recommendation Nos. 10, 11)	17
Recommendations.....	18
Management Comments and OIG Analysis	19
Appendices	
Appendix A: Purpose, Scope, and Methodology	22
Appendix B: Management Response to Draft	24
Appendix C: Recommendations from OIG Report #OIG-10-05.....	28
Appendix D: Major Contributors to This Report.....	30
Appendix E: Report Distribution.....	31

Contents

Abbreviations

AMSP	Area Maritime Security Plan
COTP	Captain of the Port
ERB	Executive Review Board
GMS	Grants Management System
IA	Office of Intelligence and Analysis
IAIP	Information Analysis and Infrastructure Protection Directorate
IP	Office of Infrastructure Protection
MTSA	Maritime Transportation Security Act of 2002
NRP	National Review Panel
ODP	Office of Domestic Preparedness
OGT	Office of Grants and Training
OIG	Office of Inspector General
SLGCP	Office of State and Local Government Coordination and Preparedness
USCG	United States Coast Guard

Executive Summary

In October 2005, Congress directed the Inspector General to review the steps DHS has taken to comply with recommendations contained in the Inspector General's January 2005 report, *Review of the Port Security Grant Program* (OIG-05-10).¹ In that report, our office made 12 recommendations to DHS to address issues involving the strategic direction of the program, the evaluation and selection of grant awards, funding private sector projects, the status of funds, and the dichotomy between two approaches DHS used to fund projects in the second round. Because five recommendations were fundamental to the effectiveness of the program, we strongly encouraged DHS to implement our recommendations before proceeding with the next round of port security grants.²

DHS implemented our recommendations in time to improve the administration and effectiveness of the fifth and most recent round of port security grants, which totaled \$142 million for 132 projects. DHS reshaped the program to make it more strategic and more risk-based by: (1) directing funds to the nation's 66 highest risk ports using a risk-based formula and tiering process; (2) modifying the eligibility criteria; (3) instituting a new funding allocation model; and, (4) implementing a complex scoring methodology to process and rank the results of the field and national reviews as well as relative risk reduction data with more precision. The Office of Infrastructure Protection (IP) became actively involved in the program through its development of the risk-based formula, thereby filling an important and much needed role. Grantees reduced the outstanding balance of unspent funds from the first three rounds by more than \$190 million since our last report.

Despite these positive developments, DHS has not entirely eliminated the issues that led to our recommendations. The revised selection and evaluation process ranks all of the projects, but does not include a minimum score threshold to differentiate unworthy projects from worthy ones. What the actual scores imply about the merits of projects, especially the funded projects, is discounted. We identified 20 projects that reviewers determined did not meet national security priorities but were funded nonetheless. The program also skipped over higher ranked projects to fund projects that it could fully fund. In addition, a handful of awarded projects reflected incomplete

¹ H.R. Rep. No. 241, 109th Cong., 1st Sess., at 40 (2005).

² Recommendations 1, 3-4, 6, and 9.

scores or data. Field reviewers' perceptions about projects, as reflected in their scores and rankings, suggest that they still have widely varying opinions about how well projects are satisfying program criteria. Finally, although DHS clarified its policy on funding private sector projects, this policy falls short of addressing the prudence of funding certain projects.

We closed the 12 recommendations in our first report based upon evidence provided by DHS showing satisfactory corrective actions. In this review, we note that DHS continues to address the issues that we raised. However, our work on the present report suggests that there are additional actions that DHS should take to improve the administration and effectiveness of the port security program.

We are recommending that the Under Secretary for Preparedness:

1. Establish a minimum score threshold under the new selection and evaluation process that projects must meet. Funding in the top three tiers not used as a result of implementing this minimum threshold should be reallocated to a lower tier;
2. Modify the Grants Management System (GMS) or the National Review Panel (NRP) internal database to require NRP members to enter a reason for adjusting a field review score;
3. Seek more consistent scoring by field reviewers;
4. Conduct a "pre-audit" of proposed grant award decisions; and,
5. Require private sector applicants to demonstrate how a federal grant would enhance their own security investments as a condition to receiving a grant.

Background

The purpose of the port security grant program is to reduce the vulnerability of American ports to potential terrorist attacks by enhancing facility and operational security. To date, the program has awarded over \$700 million in five rounds of grants. During our first review of the program, conducted between December 2003 and May 2004, we reviewed the design and goals of the program; potential duplication with other programs; the roles and responsibilities of participating agencies; and, the grant evaluation and selection process used during the second and third rounds of grants. The fourth round of grants began on September 13, 2004, after we concluded our fieldwork.

On January 28, 2005, our office issued its report, *Review of the Port Security Grant Program*, OIG-05-10. The report contained 12 recommendations to improve the design, management and oversight of the program (see Appendix B). DHS agreed with 11 of the 12 recommendations, and advised that it intended to use a new risk-based formula to award the FY 2005 port security grants.³ On May 17, 2005 the Inspector General testified before Congress on the status of DHS' efforts to address our recommendations.⁴

We continued to study how DHS modified this program, particularly the criteria that it would use to make grant award decisions, and whether those modifications would satisfy our recommendations. On July 1, 2005, based on DHS' action plan in implementing the recommendations, documentation pertaining to the revised grant application review process, and information obtained during discussions with program officials, we determined that DHS' Office of State and Local Government Coordination and Preparedness (SLGCP) had sufficiently responded to all 12 of the recommendations in our report.⁵ SLGCP's Office of Domestic Preparedness (ODP), which later became the Office of Grants and Training (OGT), assumed administrative responsibility for the program beginning with round five.⁶

On July 14, 2005, Senator Kerry introduced legislation to require the OIG to issue a report to the Homeland Security Committees of the House and the Senate on steps SLGCP has taken to comply with the recommendations contained in our report.⁷ Anticipating the enactment of the *Homeland Security Appropriations Act of 2006*, the OIG initiated a review of DHS' corrective actions and changes to the program on September 6, 2005.⁸

³ On May 12, 2005, DHS announced the availability of \$142 million for round five of the port security grant program. Actual grant awards totaled \$141,969,968. An additional \$3,887,661 was awarded specifically for ferry security through the Transit Security Grant Program.

⁴ *Hearing on Port Security Before the Senate Comm. on Commerce, Science, and Transportation*, 109th Cong., 1st Sess. (2005) (statement of Richard L. Skinner, Acting Inspector General, Office of Inspector General, Dept. of Homeland Security).

⁵ On July 13, 2005, Secretary Chertoff reorganized DHS. As part of that reorganization, SLGCP was divided. The Office of State and Local Government Coordination was realigned under the Assistant Secretary for Congressional and Intergovernmental Affairs. The Office of Domestic Preparedness was renamed the Office of Grants and Training, which is led by an Assistant Secretary who reports to the Under Secretary for Preparedness.

⁶ The Transportation Security Administration, along with the Maritime Administration and the U.S. Coast Guard (USCG) managed the first four rounds of the Port Security Grant Program. Responsibility for the program was transferred to SLGCP prior to round five. SLGCP carried out the OIG's previous recommendations.

⁷ Amendment No. 1162 to H.R. 2360, 109th Cong., 1st Sess., at 40 (2005), *DHS Appropriations for FY 2006*.

⁸ H.R. Rep. No. 241, 109th Cong., 1st Sess., at 40 (2005). The report directed the Inspector General to "review the steps the Department has taken to comply with recommendations contained in the Inspector General's report on port security

Results of Review

The Port Security Grant Program is More Strategic (Prior Report Recommendation Nos. 1, 12)

Previously, we reported that the Port Security Grant Program's strategic effectiveness was hindered by attempts to reconcile three competing requirements or approaches: the competitive program mandated by Congress through its appropriations; the *Maritime Transportation Security Act's* (MTSA) grant authority (which was not funded through appropriations) and risk-based decision-making. These competitive approaches were clouding the direction of the program. We recommended that SLGCP determine to what extent the program should incorporate MTSA requirements; and, seek clarification on the legislative intent for the program (sector-specific vs. larger infrastructure protection initiatives) as well as construct a unified program (policy, purpose, process, and eligibility) to comply with that intent. We subsequently closed these recommendations based on SLGCP's plan to redesign the program using a risk-based prioritization strategy that retained competition, included MTSA requirements where possible, and incorporated more risk data into its grant decision-making.

During the period covered by our first review and for the grants covered by this follow up review, Congress had not funded the MTSA port security grant program.⁹ Nevertheless, because applicants must be MTSA-regulated entities, OGT expanded authorized program expenditures to include MTSA-compliant security measures such as canine explosive detection programs, which would otherwise not have been funded. OGT did not incorporate MTSA features such as its 25 percent cash match requirement. Program officials reported receiving little feedback from Congress on the direction of round five. OGT redesigned the program by intertwining a "fair and equitable" process of evaluating grant applications with a funding allocation model that captures the essential elements of risk: vulnerability,

grants (OIG-05-10) [and submit a report] to the House and Senate Committees on Appropriations; the Senate Committee on Commerce, Science, and Transportation; the Senate Committee on Homeland Security and Government Affairs; and the House Committee on Homeland Security no later than February 10, 2006." Congress passed the *DHS Appropriations Act of 2006* on October 18, 2005. Pub. L. No. 109-90, 119 Stat. 2064 (2005).

⁹ On October 18, 2005, for the first time, Congress did fund the MTSA. The changes that action may have on future port security grants were not within the scope of this review.

consequence, and threat.¹⁰ OGT's objectives under the new approach were twofold: (1) allocate grant dollars roughly in proportion with the overall risk environment at the eligible port areas; and (2) select projects for funding that presented the best risk reduction potential against high-priority threats. The intent was to raise the overall bar of preparedness for the national priority threats across all eligible port areas, while still targeting dollars to the high-priority risk environments.¹¹

The new prioritization strategy included: (1) using a complex risk algorithm to identify 66 ports from a list of 129 ports across the country; (2) dividing the 66 ports into risk tiers; (3) allocating funds to each tier; (4) revising the evaluation criteria; and (5) employing a complex scoring methodology to optimize the selection of projects within tiers. Program officials considered three options before deciding how to allocate funds. We studied these changes, particularly, the underlying data in the risk formula used to identify and rank the 66 ports, and the program's new model for allocating funds to the ports. Program officials synchronized funding allocations with the results of the risk formula. These are major enhancements that substantially improve the strategic effectiveness of the program.

Program officials advised that DHS is considering whether to expand the number of eligible ports to 118. This contradicts the strategic direction OGT established in round five. However, if the new risk formula, scoring methodology, and number of tiers remain intact, extending eligibility to 52 additional ports should not affect the program's strategic focus because of its competitive nature. Furthermore, these new ports would have to compete against the 41 existing Tier IV port areas. In round five, OGT only funded projects from half of the 66 ports.

As the program continues to evolve, an important challenge that DHS should undertake is the measurement of its impact. Because DHS has awarded over \$700 million in five rounds of grants, it has "raised the overall bar of preparedness," but it is not clear that DHS knows how much actual risk reduction has been achieved. Data contained in area maritime security plans, facility security plans, and port-wide vulnerability assessments may serve as valuable measuring sticks in this evaluation.

¹⁰ Public Law 108-334, 118 Stat. 1298 (2004), *DHS Appropriations Act of 2005*, stipulated that "\$150,000,000 shall be for port security grants, which shall be distributed under the same terms and conditions as provided for under Public Law 107-117, 115 Stat. 2230 (2002)," which called for a fair and equitable program.

¹¹ FY 2005 Port Security Grant Program Risk Tier Strategy, guidance from OGT.

The Office of Infrastructure Protection Fills Necessary Role (Prior Report Recommendation No. 2)

We reported that the program did not have the benefit of critical infrastructure protection information developed by DHS' former Information Analysis and Infrastructure Protection Directorate (IAIP).¹² Therefore, port security grants were awarded without basic data about national port security priorities. We recommended that SLGCP incorporate critical infrastructure and key asset data from IAIP into the evaluation of proposed port security projects. Among the changes to consider were adding an IAIP official to the Executive Review Board (ERB); using the IAIP national asset database to identify critical facilities in need of mitigation with a view toward soliciting proposals from these facilities; and, collaborating with IAIP in an outreach program to improve the quality of vulnerability assessments and proposals. Subsequently, we closed this recommendation after confirming that SLGCP was seeking IAIP's assistance in the evaluation process and in the development of a standardized risk assessment methodology for prioritizing critical infrastructure and key asset information.

OGT's program officials are leveraging expertise within the Office of Infrastructure Protection (IP). IP made a significant contribution to the redesign of the program by creating the risk-based formula for identifying and ranking the eligible ports. The formula introduced consequence, vulnerability, and threat information that reviewers in previous rounds did not have. Program officials are planning to include more critical infrastructure data in the future. IP analysts also participated on the National Review Panel (NRP). IP's increased participation is one of the program's key developments, and a good example for other infrastructure grant programs to emulate.

Improved Evaluation and Selection Process Reduces, but does not Eliminate, Concerns about Funding Unworthy Projects (Prior Report Recommendation Nos. 3 – 5)

In rounds two and three, grant award decisions were made with the intent to expend all available funding and spread funds to as many applicants as possible. DHS funded projects that received lower scores from its

¹² At the time, IAIP consisted of two main offices, the Office of Information Analysis (IA) and the Office of Infrastructure Protection (IP). When DHS reorganized in 2005, IA became the Office of Intelligence and Analysis. IP, which retained its name, was moved to the Preparedness Directorate. The Assistant Secretary for Infrastructure Protection leads IP.

evaluators, raising questions about the merits of those projects. We recommended that SLGCP consider changing the weighting of the evaluation criteria, with greater emphasis placed on the criteria that reduce critical vulnerabilities; cease the practice of funding projects that do not meet the definition of a Priority I project, consider implementing a scoring threshold that ensures that projects not meeting that threshold are not funded; and, consider seeking a change in appropriations language to have these grant funds designated as “no-year monies” to reduce the pressure to fund lower ranked projects; and, require reviewers to document their decisions in the Grants Management System (GMS), particularly when they are inconsistent with recommendations from a lower level of review.¹³

Subsequently, we closed these recommendations because program officials were planning to implement new criteria, incorporate a weighted approach in evaluating projects, apply risk-based weightings in the selection of ports, and abandon the “Priority I” designation. SLGCP concurred that reviewer comments should be mandatory when there is disagreement between any of the review levels. SLGCP said this would be a requirement in GMS as part of the FY 2005 evaluation process. SLGCP was in the process of developing enhanced field- and national-level review guidance.

In round five, OGT incorporated several substantive changes into the application evaluation, selection, and award process. These changes included creating risk tiers for strategic ports, revising eligibility criteria, and implementing a new project scoring system.

First, OGT abandoned the Priority I, II, and III designations in favor of a new methodology. For the first time, OGT identified, ranked, and tiered ports based on risk, and addressed the need to target critical vulnerabilities with greater transparency and less confusion. The tiers, which were established using IP’s data and analysis, grouped eligible ports into four categories according to the greatest security risks. OGT allocated more funds to the nation’s highest risk ports (see Table 1). In round five, entities within the respective tiers competed against each other for port security grants.

¹³ Prior to round five, reviewers divided projects into Priority I, Priority II, or Priority III projects. Priority I projects were ranked the highest and funded. Priority II projects were acceptable, but the proposed approach did not have enough information and they were not funded. Priority III projects were considered weak projects and not funded.

Table 1: Round Five Funding Allocation to Tiers

Tier	# of Ports	Total Amount for Tier	Average Amount per Port*
Tier I	2	\$41,944,674	\$20,972,337
Tier II	3	\$20,747,921	\$6,915,973
Tier III	20	\$62,260,946	\$3,113,047
Tier IV	41	\$17,016,426	\$415,034

*This column reflects how much each port would have received if there was no competition and the funds were divided evenly amongst ports in each tier.

Second, OGT revised the project evaluation criteria, assigning extra weight to projects that reduced three critical vulnerabilities constituting the greatest threats to port security: improvised explosive devices (IEDs) delivered via small craft, underwater, and in vehicles on ferries. OGT condensed the six criteria used to evaluate projects in earlier rounds to four by eliminating the criteria measuring the “extent of actions taken thus far” and whether “the approach is comprehensive and detailed,” and clarifying the remaining criteria. Reviewers scored projects using a scale of one (lowest) to five (highest) for responsiveness (see Table 2).

Table 2: Field Review Scoring System

Criterion	Score
Risk reduction potential (national priority threat)	20 pts*
Prevention / detection of underwater IED attacks (10 pts)	
Prevention / detection of IED attacks by small craft (10 pts)	
Prevention / detection of vehicle borne IEDS on ferries (10 pts)	
Consistency with Area Maritime Security Plan	5 pts
Applicability to local security priorities	5 pts
Potential risk reduction for least cost (cost effectiveness)	5 pts
<i>Total possible score</i>	35 points

*The NRP subsequently awarded points for either a combination of underwater and small craft attacks or vehicle borne IEDs, but not both.

The most critical criterion measured a project’s risk reduction potential (the national priority threat) and accounted for a total possible score of 20 points, or 57 percent of the field review score. The remaining criteria, comprising 15 points, measured local security priorities and cost. By weighting the score in this manner, the program showed a preference for projects that supported the national security priority.

Third, once the field and national reviews had scored and ranked the projects, program officials passed the individual ratings through an

extremely complex scoring system.¹⁴ The system calculated a preliminary project score (PPS) by weighing the four criteria according to the following formula:

$$(2 \times \text{Criterion 1}) + (4 \times \text{Criterion 2}) + (4 \times \text{Criterion 3}) + (4 \times \text{Criterion 4})$$

Then the scoring system combined multiple calculations to produce a final project score and ranking for every project. The final project score consisted mostly of the PPS, but also included the priority score adjustment (the project ranking relative to the Captain of the Port's (COTP) top-ranked project in each port), and the IP priority adjustments (the project's port ranking relative to the top-ranked port in each tier).

Program administrators should modify the new scoring system to better distinguish worthy from unworthy projects

The sophisticated, and improved, scoring methodology used to rank all of the projects during the evaluation and selection process should include a minimum scoring threshold in order to distinguish worthy from unworthy projects. The absence of a minimum scoring threshold and the practice of funding “down the list” until funds are exhausted resulted in the program funding projects that provided no national threat priority reduction or were ranked below other projects. This raises concerns as to whether the scoring system gave enough weight to the risk reduction criterion. A greater concern, however, is that the process did not truly identify worthy projects because the program did not establish a minimum standard that applicants must meet in order to be eligible for funding. As we stated in our first report, projects not meeting such a threshold should not be funded.

Program administrators ranked the projects but did not identify a score within each tier that worthy projects had to attain to receive funding. OGT funded projects as they were ranked until the tier's designated funds were exhausted (grant funds were not designated as “no-year monies.”) OGT also made it a policy in round five to only fund projects in their entirety. Consequently, OGT skipped over higher ranked projects in order to find projects with costs that did not exceed the remaining funds.

The new scoring system reduces the weight given to the national priority threat criterion from 57 percent of all four criteria constituting the risk

¹⁴ OGT contracted with Digital Sandbox, an enterprise risk management software company, to develop the new project scoring and ranking system.

reduction potential point total to 40 percent of the four criteria when calculating the PPS. Diminishing the weight of the first criterion increases the likelihood that a project receiving zero points could accumulate enough points from the three remaining criteria, along with the COTP priority score and IP's port risk score, to bolster its ranking and receive funding. Of the 132 awarded projects, reviewers rated 20 projects "not applicable" or non-responsive to any subcategory of the national priority threat.¹⁵ In some cases, these projects with a score of zero for all three elements making up the national priority threat reduction criterion received total scores as low as seven or eight out of the possible 35 points. These projects received funding totaling \$29.3 million, more than 20 percent of the awarded grant funds.

Examples of awarded projects that received no points for national priority threat reduction

Grant Recipient A, project #2, access control, grant: \$65,000, score: 8.

The applicant proposed installation of card readers on critical buildings and upgrades to the current access control system software to accommodate the "current proximity card ID system." The project scored zeros for all aspects of the national priority threat, and twos and a four for the local security priorities. The field review team provided little explanation for its scoring of this project, simply stating that the project had a "limited impact in addressing AMSP priorities," and was "limited in addressing other priorities," but that it "offer[ed] significant cost benefit." Nonetheless, the field recommended full funding. The NRP agreed with field comments, increased the project's rank by two, and did not elaborate. The project's low responsiveness to almost all criteria, in particular the heavily weighted national priority threat leads us to question whether the scoring system is effective.

Grant Recipient B, project #3, secondary gates, grant: \$326,500, score: 12.

The applicant proposed installation of crash-proof gates and crash barriers at all secondary gates to deter vehicle and pedestrian attacks. The applicant stated that the gates are not necessarily open at all times, but are used frequently. The field review team stated that this project would not have any impact on the national priority threat. The project scored well on local security priorities and on cost benefit. The NRP agreed with the field's assessment, and increased the project's rank by one, stating that the project moved up in rank "due to denial of [another] application." The project was funded with a relatively low overall score, and again raises concerns as to why it received funding, given that it scored zeros in all aspects of the first and most critical criterion.

¹⁵ Ninety-five percent of the projects that scored zero for the national priority threat fell into the top two risk tiers. None of the awarded projects in the lowest risk tier scored zeros for responsiveness to every component of the national priority threat. In other words, the funded projects in the lower risk tiers scored, on average, higher than those in the top tiers.

As a result of the grant decision-making policies noted above, these and other lower ranked projects were funded. A minimum threshold would reduce the chances of funding lower ranked or questionable projects. In round five, applicants proposed a total of 543 projects. All 543 projects were ranked based on their scores. Due to ties, the lowest ranked project was the 465th project. The program funded 132 projects. Within each tier, the funded projects contained a variety of scores, tier rankings, and overall rankings.

Table 3: Highlighted Scores by Tier

Tier	Average Score	Highest Score	“Cutline” Score*	Lowest Score	Overall Rank of Lowest Score**
I	64.09	116.16	56.63	50.05	249 th
II	96.25	140.59	91.55	50.03	374 th
III	103.59	125.94	93.63	77.24	184 th
IV	102.46	121.7	100.02	81.52	205 th

* This is the score of the last project funded in order of its rank.

**Overall rank refers to a project’s rank across all tiers, which does not necessarily correspond with a project’s rank within a tier.

As a result of skipping projects, many lower ranked projects were funded:

- In Tier I, the top 36 projects were funded (projects ranked 35th and 36th were ranked 259th overall), as was the 47th ranked project (249th overall) in that tier. Tier I projects had a far lower average score than in the other three tiers, despite the added weight given to those projects for belonging to applicants located in the top tier. For example, 31 Tier I projects scored lower than the average score for Tier II projects. The overall quality or benefits of Tier I projects did not match that of projects in less critical tiers, yet the program allocated the largest portion of funds (\$42 million) to this tier.
- In Tier II, the top 14 projects were funded, but the next seven funded projects were ranked 16th, 18th, 19th, 27th (230th overall), 29th (277th overall), 36th (348th overall), and 38th (374th overall). The last project had a “preliminary score” of 28, or one of the lowest scores given by reviewers. A “preliminary score weights the four criteria and is one of the key parts of the project’s total score.
- In Tier III, the top 48 projects were funded, as was the 50th and 76th ranked projects in that tier. A total of 25 projects were skipped to reach the 76th

ranked project, including the 56th (70th overall), 58th (66th overall), and 61 (86th overall).

- In Tier IV, 24 projects were funded, including the top 17 in that tier. Among the funded projects were the 31st (164th overall) and 50th (205th overall) while several higher ranked projects such as the 48th, 72nd, 73rd, and 79th were not. This tier's 18th ranked project was ranked 48th overall, but despite the applicant's 10 percent match, there was not enough funding allocated to this tier to fund the requested grant of \$7.9 million.

The range of “cutline” scores—56.63 (Tier I) to 100.02 (Tier IV)—is another disparity that could be eliminated by implementing a scoring threshold.

With respect to the 20 projects identified above, program officials stated that it was possible and appropriate for a project with a low score in the national threat priority reduction criterion to score highly enough in the three remaining criteria to end up with a high preliminary project score. They also pointed out that most of these projects were in high risk port areas, meaning they received a high port risk score, and this helped those projects rise above their tier's funding cut line. Officials acknowledged that the lower ranked and funded projects that we identified were the result of skipping projects until a project was found that requested an amount less than the remaining dollars in the tier.

GMS revealed some anomalies for awarded projects in the form of incomplete scores or errors in reporting data.¹⁶ In most cases, the discrepancies indicated a disconnection between the information provided by the field review team and the information as assessed by the national review team.

Examples of inconsistencies in the project evaluation and selection process

Grant Recipient C, project #3, security lighting with solar battery back-up, grant \$136,000, field review score: 8.

The applicant proposed introducing security lighting on a bridge where there was previously no lighting. Field reviewers stated that this project was “not applicable” to and “d[id] not address” the national priority threat. They gave the project zeros for all aspects of this criterion, and a total score of nine. In its database and on the final spreadsheet, the NRP listed the field review scores as five, five, and zero for the first criterion. The panel did not provide any additional comments or explanation for

¹⁶ DHS contracted the administration of the Grants Management System with Booz Allen Hamilton, a global strategy and technology consulting firm.

changing these scores. The discrepancies in reported scores and the lack of explanation for amending them, particularly because this project was funded despite low scores, raises concerns about the integrity of the process.

Grant Recipient D, project #2, portable generators, grant \$3,110, field review score 15.

The field review team stated that this portable generator system was intended to power the lighting system proposed in a separate project (#1) from the same applicant, and that it “should not be approved unless project #1 is also approved.” The project received average to moderate scores for most criteria. The NRP agreed with the field’s assessment and did not elaborate. Project #1 was rejected, but against the field review team’s recommendation, project #2 was awarded. The NRP did not explain why it did not heed the field’s recommendation. The fact that portable generators were funded, even though the lighting system they would power was not funded, also raises concerns about the process.

Grant Recipient E, project #1, interoperability expansion central dispatch, requested but not granted \$2,044,240, field review score 25.

The field review gave this project a high rank and score, and described in detail how it would address national and local security priorities, stating that “The layered security provided by implementing communication interoperability systems dramatically reduces the risk for all these critical infrastructures and enables all local law enforcement, as well as Federal and industrial agencies to respond to any potential threats or breaches of security.” National reviewers appeared to concur with this assessment, and even increased the project’s rank. Given the project’s high rank and score, particularly with regard to the weighted national security priorities, it is unclear why this project was not funded.

Program officials were reviewing the project anomalies, but did not respond in time for the issuance of our draft report. We anticipate that their explanations will show that these are not systemic problems, but they nonetheless highlight internal control weaknesses that need to be corrected in the evaluation process.

Documentation of reviewers’ evaluation and decision-making in round five improved, containing more detail than in rounds two and three. Field and national reviewers also demonstrated greater consistency in their assessments and took more care to justify their decisions. Unlike in earlier rounds, there were fewer instances of the NRP upgrading or downgrading the field review’s scores without providing any justification. For example, in one application for floating protective barriers, the national review downgraded the project scores for national priority threat reduction noting, “Criteria 1.2 – Prevention [changed from] 5 to 4 – provides good physical

and visual deterrent, but would not [prevent] larger craft. Detection [changed from] 5 to 2 – does not provide any communication that attack is imminent.” In this and other examples, the NRP presented its reasoning for altering scores.

However, in some cases reviewer justifications for the rank and score assigned to applications still lacked detail. Field reviewers provided sparse comments and little insight as to how a project would address critical security needs, stating only that they did or did not “recommend funding.” NRP members depend on the USCG’s local knowledge and expertise to make informed evaluations and funding decisions, and thus the lack of explanations from the field could affect their decision-making. Similarly, while NRP comments were more evident than in previous rounds, they remained thin in cases of non-funded projects. For example, NRP explanations for why projects that seemed worthy of funding were not funded frequently state, “not funded” or “fell below tier line,” which are not informative evaluations. This was not entirely unexpected, given that they thought projects falling below the tier line would not be funded.

Overall, the project evaluation and selection process employed in round five demonstrated marked improvement. OGT set forth specific national priorities and implemented a risk-based prioritization system. However, the practice of funding projects that were not scored as responsive to program priorities in order to expend all available funds is a concern. The practice of funding projects that reviewers score as marginal continues to be an issue for the program. As OGT develops program guidance for round six, it should reconsider adopting a minimum score that separates worthy from unworthy projects.

Field Reviewers Scored Projects Differently (Prior Report Recommendation Nos. 6 – 8)

In rounds two and three, headquarters and field reviewers did not always share a common understanding of program objectives or eligibility criteria. We recommended that SLGCP develop parameters that define applicant eligibility under the “nationally important economic port or terminal,” “responsible for movement of a high number of passengers,” and “responsible for the movement of hazardous cargo” criteria; communicate information to field reviewers to educate them on eligibility and improve dissemination of “lessons learned” at all levels of review; and evaluate timeframes for reviewing applications with an emphasis on providing more

time for review in the field and by the Executive Review Board (ERB). We closed those recommendations because SLGCP was (1) working with IAIP and USCG to develop clearly defined parameters for port eligibility, (2) developing enhanced guidance on eligibility guidelines using lessons learned from previous rounds, and (3) developing a more efficient process for vetting projects, which included eliminating one level of review (the ERB).

In round five, OGT evaluated the nation's 129 largest volume ports using a risk-based formula that analyzed a port's consequence, vulnerability, and threat.¹⁷ Based on this evaluation, the program identified 66 eligible port areas. OGT identified eligible applicants as: (1) owners/operators of federally regulated public or private ports, terminals, U.S. inspected passenger vessels, or ferries; (2) port authorities, and/or State and local agencies that provide layered security protection to federally regulated entities; and (3) consortia composed of local stakeholder groups representing federally regulated ports, terminals, U.S. inspected passenger vessels, or ferries.¹⁸ Program administrators communicated eligibility requirements to the field review teams, improving field-level knowledge of application prerequisites.¹⁹ The newly-instituted eligibility requirements eliminated the previous confusion resulting from poorly defined eligibility criteria, such as whether an applicant represented a nationally critical port.

Subjectivity remains inherent in this process, which relies heavily upon the judgment of the field reviewers. As a result, disparities existed between project scores submitted by field review teams in various ports, suggesting that they are not assessing projects equally. For example, the Houston port area project scores ranged from 9 (lowest) to 30 (highest). In the same port risk tier, the New York/New Jersey port area project scores ranged from a low of 3 to a high of 17. This disparity in project scores for like-port areas (in terms of risk) raises concerns about the basis for field review scores and how reviewers are judging projects against the criteria. The accompanying explanations for reviewer scores in the field evaluation sheets were straightforward and did not provide any information that could explain the differences. We did not conduct a project-by-project analysis to determine whether the reviewers were using similar approaches to scoring.

¹⁷ Program Highlights: FY 2005 Port Security Grant Program. For the purposes of this formula, "consequence" considered "people, economic, national security, and port-specific special considerations (hazardous materials, oil)." "Vulnerability" considered "the distance from open water, number of port calls, and presence of tankers." "Threat" included credible threats and incidents, less credible threats and incidents, and vessels of interest information.

¹⁸ Program Highlights: FY 2005 Port Security Grant Program.

¹⁹ Port Security Grants – Round 5 Program Guidance Document (For U.S. Coast Guard Field Evaluators/Reviewers)

The revised evaluation and selection process saved time. The elimination of the ERB removed a layer of review and improved timeframes from previous rounds. On the other hand, these modifications did not ensure that reviewers would include necessary commentary and justifications for recommendations on the applications. Program administrators should continue to enhance the standardization of field review scoring methodology and take steps to ensure that field and national reviewers will provide detailed explanations in the future. Finally, program administrators should implement an internal quality assurance review, or “pre-audit” – possibly by a grants administrator not directly involved in the program – to help prevent project anomalies in the future and ensure the program’s credibility.

Private Sector Policy Should Address Prudence of Funding Certain Projects (Prior Report Recommendation No. 9)

Another dilemma confronting the program related to the circumstances under which private entities might obtain grant funding. DHS did not have a formal policy to govern financial assistance to private entities, including those that own and operate high-risk port facilities. Many grants to private companies were for basic security measures that should have been considered as normal costs of doing business, and some were within their financial means. We recommended that SLGCP clarify its policy on funding private sector projects. In the absence of such policy, and if funding private sector projects is continued, we recommended that SLGCP: (a) examine private sector projects to preclude the funding of cost of business expenses; (b) develop financial eligibility criteria, including an income test or cost-benefit analysis; and (c) consider giving greater preference to projects that are submitted jointly by private and public entities.

We closed this recommendation because SLGCP said it would implement two significant changes. First, it announced that it would require a 50 percent cash match, thereby securing a greater commitment from companies while also demonstrating a willingness to help pay for costs to comply with MTSA. Second, it rendered Fortune 500 companies ineligible in round four. As a result, grant awards to private companies in that round totaled \$6.3 million, the lowest amount of any round.

OGT implemented this policy in round five. Private companies proposed fewer projects than public entities, and received \$8.2 million. However, the presence of a matching requirement does not fully address the question of

whether DHS will consider the prudence of funding certain private sector projects. The program restored eligibility for Fortune 500 companies in round five, placing less emphasis again on the company's financial condition. Round five contained far fewer questionable grants like the ones we previously reported, but the program has not ceased this practice altogether. For example, a Fortune 500 refinery received a port security grant in round five totaling almost \$1 million for fencing and surveillance upgrades at a refinery located in a major port. It did put up the same amount in matching funds. This company recently reported 3rd quarter net income in excess of \$1.2 billion. We remained concerned about the absence of more specific guidance on security measures proposed by private companies that are capable of paying for them, and what measures they should pay for.

Also, there is the question of how well the project matches program criteria. The program is supposed to identify projects that address national port security priorities and provide security enhancements that are most likely to help sustain overall port operations. Private sector projects can score poorly against these criteria but well enough on the local security priority criteria to receive funding. In the case above, the risk factor of the port where the project was located helped the project's overall ranking during the evaluation process. Of the 20 projects that received zeros in the national threat priority criteria, 12 were private sector projects. They received enough points in other criteria to receive funding totaling \$4.2 million.

Should DHS elect not to reconsider using financial criteria, it should at least require companies and public entities to demonstrate how their own security investments would be leveraged by a federal grant.

Balance of Unspent Funds is Declining (Prior Report Recommendation Nos. 10, 11)

As of September 30, 2004, grant recipients had spent only a small portion of their awards. Of the \$515 million awarded between June 2002 and December 2003, including the \$75 million provided in DHS' Urban Area Security Initiative, grant recipients had expended only \$107 million, or 21 percent. We determined that many of the recipients were simply not prepared to put their grant funds to use and DHS did not have sufficient resources to monitor the progress—or lack thereof—of individual projects. We recommended that SLGCP accelerate the acquisition of more information from applicants about the scope of their projects and ensure that the program has sufficient operational expertise to administer the program after the award

is made. We subsequently closed these recommendations because of ongoing efforts to update the guidance for applicants, and planned creation of the Transportation Infrastructure Security Division within SLGCP.

Our recommendations were designed to address factors contributing to slow spending. Round five will be the first round to fully benefit from DHS' actions. SLGCP issued the FY2005 Port Security Program Guidelines and Application Kit, which contained specific directions for applicants including information required in the project narrative, individual project plan, and detailed budgets. Compared to our observations of rounds two and three, round five reviewers noted far fewer concerns in GMS about the scope and cost of projects. Of the 43 project files we reviewed in depth, none revealed that the applicant provided insufficient information about scope and cost.

Program officials extended project periods to 30 months in round five, because several entities received awards in more than one round. Administrators should monitor entities that receive multiple grants or have not drawn down any funds. A total of 20 round two projects totaling \$13.7 million and 32 round three projects totaling \$35.8 million have not drawn down any of their funds. To that end, six TSA personnel were transferred to OGT to help staff its Transportation Infrastructure Security Division and oversee the program. Despite these projects, the balance of unspent funds has declined since our first report, even when taking into consideration round four. At the time of our report, the balance of unspent funds for the first three rounds was \$347.4 million. Today, the balance is \$179.5 million, or \$222.3 million including round four.

Recommendations

DHS has worked to address the issues we raised in our January 2005 report. However, our follow up review suggests that there are additional actions that DHS should take to continue to improve the administration and effectiveness of the program. Accordingly, we recommend that the Under Secretary for Preparedness:

1. Establish a minimum threshold under the new selection and evaluation process that projects must meet to become eligible for funding. Funding in the top three tiers not used as a result of implementing a minimum threshold should be reallocated to a lower tier.

-
2. Modify the Grants Management System (GMS) to require National Review Panel (NRP) members to enter a reason for adjusting a field review score.
 3. Seek more consistent scoring by field reviewers.
 4. Conduct a “pre-audit” of proposed grant award decisions.
 5. As a condition of receiving a grant, require private sector applicants to demonstrate how a federal grant would enhance their own security investments.

Management Comments and OIG Analysis

We issued our draft report on January 6, 2006. Below is a summary of DHS’ response to our recommendations, and our analysis of the response. A copy of DHS’ response in its entirety is recorded in Appendix B.

Recommendation 1: Establish a minimum threshold under the new selection and evaluation process that projects must meet to become eligible for funding. Funding in the top three tiers not used as a result of implementing a minimum threshold should be reallocated to a lower tier.

DHS is still considering whether to implement a minimum score threshold for projects to receive funding. DHS stated that the program must take into account that even if a project in a lower risk tier receives a high score, this must be balanced against the fact that a project in a higher risk tier receiving a lower individual score may still achieve greater overall risk reduction. Finally, DHS believes that the lack of responsiveness to the national priority threat was a result of some ports’ poor understanding of the national priority threat requirement and its impact on application rank, and stated that enhanced guidance in round six will better explain this emphasis.

Since DHS is still considering whether to implement a threshold, we consider the recommendation unresolved and open. In round five, the program improved the process of allocating funds based on risk, and we agree that enhanced guidance may improve responsiveness of project applications to the national priority threat. However, improving guidance and emphasizing the national priority threat does not fully address the problem of lower-scored projects receiving awards. We believe that comparing project scores across

tiers is fair and prudent, as relative port risk scores are already accounted for in the formula that generates a project's individual final score. We will await additional information from OGT regarding how it intends to ensure that low scoring projects do not continue to receive funding.

Recommendation 1 – Unresolved – Open

Recommendation 2: Modify the Grants Management System (GMS) to require National Review Panel (NRP) members to enter a reason for adjusting a field review score.

DHS agreed that in round five the review process did not fully document NRP comments and justifications for award decisions, and stated that OGT will allow panel members to denote this information in OGT's portal. DHS stated that OGT would additionally enable reviewers to access the project applications prior to convening the NRP, so that panelists may more completely represent their perspectives.

We recognize that OGT is poised to make the NRP's responsibility to document its decisions even more transparent in round six. However, we feel that OGT's proposed actions fall short of requiring that NRP members provide the reasons for their decisions. Allowing panelists the ability to capture their notes in the portal does not ensure that they will do so sufficiently to record the justifications for granting or denying awards. The relevant fields for such comments already existed in the round five review process, yet in some cases NRP members still did not utilize these fields to provide details on the reasons for their decisions. DHS should require panelists to provide justifications for its award decisions and demonstrate that the system enforces this requirement.

Recommendation 2 – Unresolved – Open

Recommendation 3: Seek more consistent scoring by field reviewers.

DHS agreed that it is necessary to ensure more consistency in the field review. DHS stated that OGT is revising round six program guidance to enhance the consistency of the field review scoring process with additional examples, templates, and guidance. This effort will be augmented by teleconferences during the review period to focus on requirements and expectations.

We concur that improved program guidance and direction to field reviewers will encourage consistency in the process. We request that OGT provide us with the Field Review Guidance for round six in order to satisfy our expectation that the revisions promote improved consistency across the field review.

Recommendation 3 – Resolved – Open

Recommendation 4: Conduct a “pre-audit” of proposed grant award decisions.

DHS recognized that the manual process of administering the program requires improvement. DHS stated that OGT is exploring information technology enhancements to automate the NRP and field review scoring processes, and the process used to generate the final list of projects to be funded. DHS advised that these changes would increase accuracy of the reported data through the review process, and enable OGT to analyze and convey program data to senior officials.

We concur that, if implemented at each level of the review, automation of the scoring and data transfer systems as described by DHS will reduce the likelihood of, and opportunity for, errors. We look forward to the execution of these technological enhancements, and ask that OGT share them with us once they have been implemented.

Recommendation 4 – Resolved – Open

Recommendation 5: As a condition of receiving a grant, require private sector applicants to demonstrate how a federal grant would enhance their own security investments.

DHS stated that in round six the program will require all applicants to exhibit the impact of conducting or not conducting the proposed project, based on risk data relative to the targeted security measure. DHS stated that this demonstration of project merit will enable the program to award projects with the greatest opportunity for risk reduction and measure the impact of an award in terms of buy down of risk.

While we agree that all applicants should be required to discuss the opportunity costs of their proposed projects, DHS’ response does not indicate whether private sector applications will undergo greater scrutiny. Instituting

this opportunity cost requirement, which calls upon applicants to demonstrate project merit, might address part of our concern about the prudence of funding certain private sector projects, but more information is needed. We request that OGT clarify what information it will seek regarding opportunity costs, how the cost data will account for other company security measures, and how those investments would be leveraged by receiving the grant.

Recommendation 5 – Unresolved – Open

In October 2005, Congress directed the Inspector General to review the steps DHS took to comply with the 12 recommendations contained in the OIG's January 2005 report, *Review of the Port Security Grant Program* (OIG-05-10). In response, our office examined the effect of DHS' implementation of the recommendations in preparation for round five of the program. Because of the timing of our first review, we did not include round four in it or in our follow up review.

In order to assess the changes DHS made for round five, our office revisited the Port Security Grant Program's strategic goals and objectives and how the grants served to protect national critical infrastructure. We reviewed numerous documents including:

- The FY2005 Port Security Grant Program Resource Binder.
- The port risk formula, which led to the selection of the 66 eligible ports and tiering methodology.
- The funding distribution model that determined the allocation of funds to each tier.
- Changes to the eligibility criteria.
- The Grant Application Kit.
- Guidance for field and national reviewers.
- Field review score sheets for the majority of the applications.
- Each port area's list of ranked projects.
- The final scoring system, which incorporated IP data and priority adjustments to produce the final project ranks.
- Current reports on the status of funds for the first four rounds.

Additionally, we scrutinized the quantified results of all funded and non-funded projects. We reviewed 43 projects in greater detail by examining documents submitted by the applicants, specific comments by field and national reviewers, and tracking project scores through the scoring system. We carried out a significant portion of our project review by viewing electronic files in OGT's Grants Management System, the National Review Panel's internal database, and via OGT's intranet portal at OGT headquarters in Washington, DC.

We discussed the redesign, management, and oversight of the program with officials from the Office of Grants and Training, the Office of Infrastructure Protection, and the U.S. Coast Guard. We assessed the coordination between the OGT's program administrators and IP. We also met with a representative

from Digital Sandbox, the contractor who developed the new scoring and ranking system.

We conducted our review between September 2005 and December 2005 under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency.

Appendix B
Management Response to Draft

Preparedness Directorate
U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

February 7, 2006

MEMORANDUM TO: Robert L. Ashbaugh
Assistant Inspector General for Inspections
and Special Reviews

FROM:  George W. Foresman
Under Secretary for Preparedness

SUBJECT: Response to Draft Inspector General Report on the
Followup Review of the Port Security Grant Program

This responds to your January 6, 2006, memorandum requesting the Preparedness Directorate's comments on the draft Office of the Inspector General report, *Followup Review of the Port Security Grant Program*. First, we sincerely appreciate the opportunity to respond to the draft report. In addition, we value the positive comments and feedback provided in the Executive Summary relating to recent program enhancement efforts. Finally, we are pleased to report that, through the Office of Grant and Training's (G&T) review of the FY 2005 process, we have already identified and begun to develop solutions to four of the five recommendations outlined in the draft IG Report. The remaining item is a matter of policy and we are taking a closer look at this matter to avoid the occurrence of anomalies in its process during FY 2006.

The attached document provides specific comments and plans of action for addressing the five recommendations contained in the draft report. Questions concerning specific comments should be addressed to Brad Shefka at 202-282-8532.

In closing, please accept our thanks for the opportunity to work alongside the Office of the Inspector General in reviewing this important program. As the Preparedness Directorate Office works toward refining its programs, the Office of the Inspector General's independent analysis of program performance greatly benefits our ability to continuously improve our activities. We look forward to continuing this partnership in the future.

Attachment

cc: Tracy Henke
Steven Pecinovsky

**Response to Recommendations Contained in the
Draft IG Report
Followup Review of the Port Security Grant Program**

Recommendation #1: Establish a minimum score threshold under the new selection and evaluation process that projects must meet. Funding in the top three tiers not used as a result of implementing this minimum threshold should be reallocated to a lower tier.

Response: The Port Security Grant Program (PSGP) has been at the forefront of the Department's efforts to embrace a resource allocation process that is based on risk. To that end, the FY 2005 PSGP was significantly enhanced through a series of policy changes that produced a more risk-informed process. Additional enhancements are planned for the FY 2006 PSGP that will further refine this focus.

The office of Grants & Training (G&T) will consider whether the IG's recommendation to implement a minimum threshold score as part of this process might benefit the program. However, consideration must be given to the fact that, even if a project in a lower risk tier achieves a very high Individual Project Score, this must be balanced against the fact that projects at ports in higher risk tiers, but with lower Individual Project Scores, may still produce a greater overall buy down in risk.

One of the problems noted in G&T's after action review of the FY 2005 PSGP process was that some ports were not as responsive to the national port security priorities identified in the grant guidance as others. In these instances, the Individual Project Scores for projects in those port areas were greatly impacted. This issue was especially notable in the highest risk tier, which included only two ports. G&T believes that, in some cases, this may have resulted from the applicant not fully understanding the requirement that projects be responsive to the national port security priorities or the impact this would have in the ranking of applications. Therefore, as part of the FY 2006 PSGP, G&T is implementing enhanced guidance that will provide applicants with a better understanding of this requirement through examples and templates.

Recommendation #2: Modify the Grants Management System (GMS) or the National Review Panel (NRP) internal database to require NRP members to enter a reason for adjusting a field review score.

Response: The FY 2005 Port Security Grant Program (PSGP) encouraged comments from the National Review Panel (NRP) and sought to make those suggestions a matter of the official record of the review process. However, during the FY 2005 NRP, the method of capturing comments was not fully automated due to the limited amount of time and resources available. The FY 2006 PSGP will address this by allowing NRP members the ability to capture notes, justifications, and decision-based logic in a set of fields encompassed within the G&T Secure Portal. G&T will also allow reviewers to access the applications and review guidance before the NRP convenes. We anticipate that this preview will foster a more refined process whereby panelists may represent their perspectives more completely and therefore allow for better capture of their comments. In addition, G&T is continuing the process of refining the guidance it

provides for all phases of the PSGP application review process to further emphasize the importance of documenting, in a standardized fashion, the decision-making process for any changes. G&T believes the combination of a more automated process and further refinement of the guidance provided to participants will mitigate this issue.

Recommendation #3: Seek more consistent scoring by field reviewers.

Response: G&T made significant changes to the PSGP application review process in FY 2005 and considers this to be a significant stride in creating a more consistent and standardized scoring approach. However, in the after action review of the process, G&T also identified the need to ensure more consistency in the Field Review element, and has made this a priority for FY 2006. As the Federal Maritime Security Coordinator at the local level, Coast Guard Captains of the Port (COTPs) managed the FY 2005 PSGP field reviews and will continue to perform this function in coordination with the appropriate Maritime Administration Regional Directors (MARAD), members of the local Area Maritime Security Committees (AMSC), State Administrative Agencies, and Homeland Security Advisors. The Field Review Guidance is currently being revised for FY 2006 to build upon last year's successes and enhance the consistency of the Field Review scoring process with additional examples, templates, and guidance. Furthermore, the process will be supported by weekly teleconferences during the review period, designed to address key requirements and expectations, as well as to ensure an enhanced opportunity for stakeholder interaction.

In addition to these program improvements, G&T also established a Port Security Track as part of its FY 2005 Regional Conferences. The Port Security Track afforded COTPs, MARAD Regional Directors, and members of the local Area Maritime Security Committees an opportunity to participate in a detailed exchange of FY 2005 lessons learned, best practices, and challenges addressed, as well as to anticipate FY 2006 program requirements. G&T believes these enhancements will build upon the changes implemented in FY 2005 and ensure more consistent field review scores.

Recommendation # 4: Conduct a "pre-audit" of proposed grant award decisions.

Response: G&T is aware that the manual process of managing the PSGP requires improvement. As a result, G&T is currently exploring a series of information technology enhancements to include:

- Automation of the NRP scoring;
- Automation of the Field Review scoring; and
- Automation of the process used to develop the final list of projects to be funded.

Assuming the availability of the resources necessary to realize these enhancements, the changes will provide an enhanced level of confidence in the movement of data through the various steps in the review process, as well as allow for the ability to scrutinize trend data and report to senior officials with respect to these programs. This will also eliminate the potential for human error inherent in a process dependent upon manual transfers of data.

Recommendation #5: Require private sector applicants to demonstrate how a federal grant would enhance their own security investments as a condition to receiving a grant.

Response: The FY 2006 Port Security Grant Program will require all applicants to elaborate on the opportunity cost of the respective project(s). In essence the applicant will be required to articulate the impact of conducting, or not conducting, the project based upon risk data relative to the targeted security enhancement. This analysis of project merit will enhance the ability to identify and invest in projects that demonstrate the greatest opportunity for risk reduction across the geo-space of the port area and measure the impact of the investment in terms of risk buy down.

We recommended that the Executive Director, Office of State and Local Government Coordination and Preparedness:

Recommendation #1: Determine to what extent the program should incorporate MTSA requirements.

Recommendation #2: Incorporate critical infrastructure and key asset data from IAIP into the evaluation of proposed port security projects. Among the changes to consider:

- The addition of an IAIP official on the Executive Review Board;
- Use of the IAIP national asset database to identify critical facilities in need of mitigation with a view toward soliciting proposals from these facilities; and
- Collaborating with IAIP in an outreach program to improve the quality of vulnerability assessments and proposals.

Recommendation #3: Consider changing the weighting of the evaluation criteria, with greater emphasis placed on the criteria that reduce critical vulnerabilities.

Recommendation #4: Cease the practice of funding projects that do not meet the definition of a Priority I project. Consider implementing a scoring threshold that ensures that projects not meeting that threshold are not funded. Consider seeking a change in appropriations language to have these grant funds designated as “no-year monies” to reduce the impetus to fund doubtful projects.

Recommendation #5: Require reviewers to document their decisions in the grants management system, particularly when they are inconsistent with recommendations from a lower level of review.

Recommendation #6: Develop parameters that define applicant eligibility under the “nationally important economic port or terminal,” “responsible for movement of a high number of passengers,” and “responsible for the movement of hazardous cargo” criteria.

Recommendation #7: Communicate information to field reviewers to educate them on eligibility. Improve dissemination of “lessons learned” at all levels of review.

Recommendation #8: Evaluate timeframes for reviewing applications with an emphasis on providing more time for review in the field by the ERB.

Recommendation #9: Clarify department policy on funding private sector projects. In the absence of such policy, and if funding private sector projects is continued: (1) examine private sector projects to preclude the funding of cost of business expenses; (2) develop financial eligibility criteria, including an income test or cost-benefit analysis; and (3) consider giving greater preference to projects that are submitted jointly by private and public entities.

Recommendation #10: Accelerate the acquisition of more information from applicants about the scope of their projects.

Recommendation #11: Ensure that the program has sufficient operational expertise to administer the program after the award is made.

Recommendation #12: Seek clarification on the legislative intent for the program (sector-specific vs. larger infrastructure protection initiatives) and construct a unified program (policy, purpose, process, and eligibility) to comply with that intent.

Appendix D
Major Contributors to This Report

William J. McCarron, Chief Inspector
Razili K. Datta, Inspector

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Assistant Secretary, Policy
Executive Secretariat
Under Secretary, Preparedness
Assistant Secretary, Office of Grants and Training
Audit Liaison, Office of Grants and Training
DHS OIG Liaison
Audit Liaison, Preparedness
DHS Public Affairs
Assistant Secretary, Office of Legislative Affairs

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

House Committee on Appropriations
Senate Committee on Appropriations
Senate Committee on Commerce, Science, and Transportation
Senate Committee on Homeland Security and Government Affairs
House Committee on Homeland Security

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.