

09 FEB 24 P 1 20

STATE PROCUREMENT OFFICE
NOTICE OF AND REQUEST FOR EXEMPTION
FROM CHAPTER 103D, STATE OF HAWAII

- 1. TO: Chief Procurement Officer
- 2. FROM: Michael D. Formby, Dept. of Transportation, Harbors Div.

Department/Division/Agency

Pursuant to §103D-102(b)(4), HRS, and Chapter 3-120, HAR, the Department requests a procurement exemption to purchase the following:

3. Description of goods, services or construction:
 The State Department of Transportation, Harbors Division (DOTH) is procuring the design, construction and installation of a Honolulu Harbor Surveillance Command Information System (H2S-CIS). DOTH desired a unique low cost system, readily integratable with the existing surveillance systems at Kewalo Basin and the State Civil Defense Emergency Operating Center (SCD-EOC). The system shall include software that integrates real time optical and radar surveillance of critical port areas and tracking of waterborne traffic as well as information from the California Integrated Seismic Network providing region-wide earthquake information--an alert system to monitor an all-threats approach to securing the Harbors. It includes two command centers located at the DOTH Pier 2 and in the Chamber level of the State Capitol. The system also provides a common operating picture in the state and counties emergency operating centers. The project concept and approach of command, control and surveillance for the Port of Honolulu is a unique Hawaiya Technologies, Inc. (HTI) concept, architecture and technical design.

4. Name of Vendor: Hawaiya Technologies, Inc. Address: 98-1809 Nahele St., Aiea, Hawaii 96701	5. Price: \$1,427,053
6. Term of Contract: From: 3-15-09 To: 10-31-09	7. Prior Exemption Ref. No. 0

8. Explanation describing how procurement by competitive means is either not practicable or not advantageous to the State: Department of Homeland Security (DHS) thru FEMA announced via its website, a competitive process of selecting projects for \$168 million in 2006 Port Security Grants. The DOTH received proposed projects from contractors responding to the DHS open announcement of the 2006 grant. The State, as an applicant for a grant, could submit up to 5 projects meeting the specific DHS/FEMA National Infrastructure Protection Plan. DOTH submitted 5 project proposals and funding the projects would be based upon a competitive FEMA evaluation process. HTI and its H2S-CIS product went through both a State screening process of projects meeting the National Infrastructure Protection Plan priorities and a Federal competitive evaluation and selection program as provided in the 2006 Grant guideline. FEMA's award of the grant was based on the State's submission of the HTI project concept, review and acceptance by the US Coast Guard. (continued on attached sheet)

9. Details of the process or procedures to be followed in selecting the vendor to ensure maximum fair and open competition as practicable:
 DOTH received and screened proposed projects from contractors responding to the DHS open announcement of the 2006 grant. DOTH selected and included proposed projects in its grant application that met the risk criteria based on national port security priorities established within the National Preparedness Goal. The DOTH then forwarded the projects for review to the Captain of the Port, USCG for field scoring based on responsiveness to the Core Program Criteria. The field scoring were forwarded to the USCG District Headquarters for review, and then to DHS/FEMA for final review and acceptance/rejection via the multi-layer competitive National Review Process. On Sept. 29, 2006, FEMA awarded 1 out of 5 projects proposed in the State's application, the project concept proposed by HTI for the implementation of their product, H2S-CIS at the Honolulu/Kalaeloa Barbers Point Harbors. FEMA competitively awarded the grant based on (continued on attached sheet)

REQUEST FOR EXEMPTION FROM CHAPTER 103D, HRS (Cont.)

10. A description of the agency's internal controls and approval requirements for the exempted procurement:
 DOTH has a full and open process to consider concepts from any entity on projects that can be included in the grant process. Upon FEMA's competitive grant announcement, the State follows the instructions provided in the Port Grant Program Guidelines and Application Kit. The proposed projects are selected based on the State's review and determination that a project concept meets the required capability of the national port security priorities established within the National Preparedness Goal, and an opportunity for the project concept to be awarded the grant and funding based on: 1) the field review by the Captain of the Port; 2) the final National review comprised of subject matter experts from G & T, USCG, Transportation Security Administration (TSA), Customs Border Patrol (CBP), OIP, and Maritime Administration (MARAD); and, 3) the timeline and availability of technologies that suit the needs of the State within the cost and time constraints of DHS/FEMA and the State. HTI's H2S-CIS went through such (continued on attached sheet)

12. A list of agency personnel, by position, who will be involved in the approval process and administration of the contract:

Name	Position	Involvement in Process	
Michael D. Formby	Deputy Director	<input checked="" type="checkbox"/> Approval	<input type="checkbox"/> Administration
Davis K. Yogi	Harbors Administrator	<input type="checkbox"/> Approval	<input checked="" type="checkbox"/> Administration
Wade Takamoto	Project Engineer	<input type="checkbox"/> Approval	<input checked="" type="checkbox"/> Administration
		<input type="checkbox"/> Approval	<input type="checkbox"/> Administration
		<input type="checkbox"/> Approval	<input type="checkbox"/> Administration
		<input type="checkbox"/> Approval	<input type="checkbox"/> Administration

13. Direct inquiries to: Department: Transportation - Harbors Div.
 Contact Name: Davis K. Yogi
 Phone Number: 587-1928
 Fax Number: 587-1982

Agency shall ensure adherence to applicable administrative and statutory requirements

14. *I certify that the information provided above is, to the best of my knowledge, true and correct.*


 Department Head

2-24-09
 Date

Reserved for SPO Use Only	
	15. Date Notice Posted <u>2/25/09</u>
The Chief Procurement Officer is in the process of reviewing this request for exemption from Chapter 103D, HRS. Submit written objections to this notice to issue an exemption from Chapter 103D, HRS, within seven calendar days or as otherwise allowed from the above posted date to: <p align="center"> Chief Procurement Officer State Procurement Office P.O. Box 119 Honolulu, Hawaii 96810-0119 </p>	

REQUEST FOR EXEMPTION FROM CHAPTER 103D, HRS (Cont.)

Chief Procurement Officer's comments:

Approval is based on the DOT's representation that the process for soliciting for projects and ultimate selection of the contractor was in conformance with requirements set forth by the Federal Government (DHS/FEMA). In this situation, the DOT was unable to follow their normal procurement process and this requires is to provide matching funds that are a requirement to secure the federal funds for this project.

This approval is for the solicitation process only, HRS section 103D-310(c) and HAR section 3-122-112, shall apply.

16.

APPROVED DISAPPROVED NO ACTION REQUIRED

Allen S. Jyer 3/9/09
Chief Procurement Officer Date

SPO-07 – Continuation of Items 8, 9, and 10

8. (Continued)

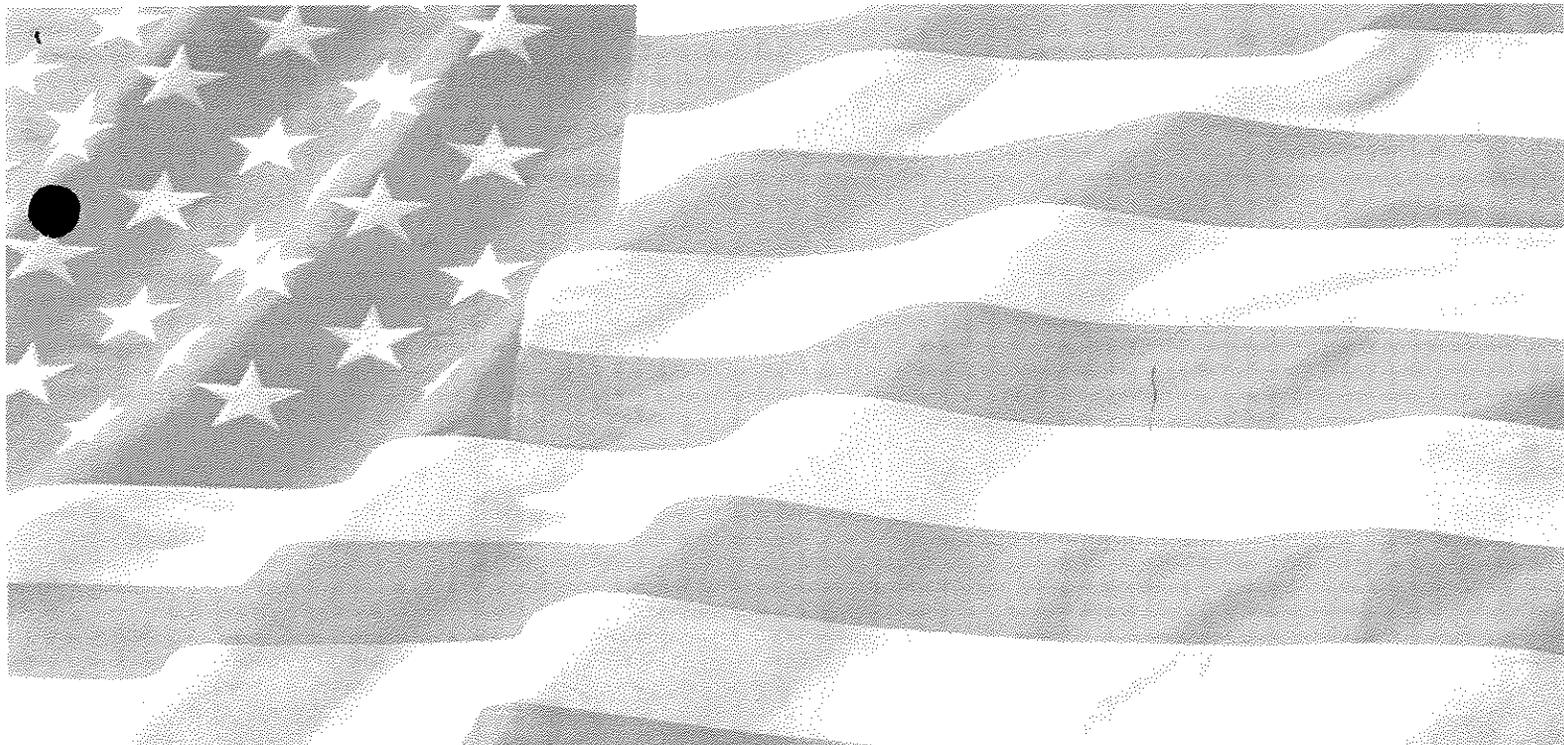
and subsequent selection and approval of a federal sole source by DHS/FEMA makes procuring another companies product by competitive means not practicable or advantageous to the State. No other entity can execute the HTI H2S-CIS concept in its technical and architectural design and as it directly relates to the dollar funding of the grant, capability, cost and proprietary information.

9. (Continued)

its rating criteria of the project, as described in the 2006 Port Grant Program Guidelines and Application Kit, and its extensive review and screening process, and as such, provided a sole source authorization and grant to HTI to implement its H2S-CIS as it has already been vetted through a fair and open competition at the federal level.

10. (Continued)

process and won the competitive award. Additionally, an assessment of the ability of a different vendor, who did propose the original concept, to implement the program within the cost and time is considered improbable/impracticable, and as such, HTI should be awarded a sole source contract as being advantageous to the State.



U.S. Department of Homeland Security
Office of Grants and Training

FY 2006 Infrastructure Protection
Program: *Port Security*

Program Guidelines and Application Kit



Foreword

I am pleased to provide these FY 2006 program guidelines and application materials for the U.S. Department of Homeland Security (DHS) Infrastructure Protection Program.

This is the first grant cycle since completion of the Department's Second Stage Review last summer and our creation of a unified Preparedness Directorate. The preparedness mission transcends the entire Department. Our approach to preparedness aggregates critical assets within DHS to support our operating components and the work of our external partners to prevent, protect against, respond to, and recover from threats to America's safety and security. The Directorate serves a strategic integration function of people, funding and programs.

The new Preparedness Directorate includes the essential work of the Department's Office of Grants and Training. In managing our grant programs, DHS is committed to supporting risk-based investments. We are equally committed to continuous innovation. As new infrastructure is built, existing facilities improved, or as our assessment of specific threats change, DHS grant programs will focus on being nimble and making high-return investments to combat terrorism.

In 2006, \$373 million is available for a package of related infrastructure protection grants. The FY 2006 Port Security Grant Program makes up \$168 million of the total infrastructure protection grant funds available. These grants are a vital tool in making our nation safer in the war against terror. They provide assistance for physical security enhancements to some of the Nation's most at-risk critical infrastructure.

For each grant, the Preparedness Directorate will rely on an integrated team of subject matter experts drawn from DHS operating components to develop, design, compete, review, and support the infrastructure grants as part of the national preparedness effort. Specifically, with respect to port security:

- The U.S. Coast Guard has the lead for assuring that the grants accomplish key objectives such as aligning our grant making to the highest risk ports and allocating funds using refined risk-based methods developed for grants. This process will hasten the development of an integrated risk-based decision making process for each port area and will support implementation of the National Infrastructure Protection Plan (NIPP) and achievement of the National Preparedness Goal.
- The Department of Homeland Security's Office of Grants and Training provides design, facilitation, coordination and financial management administration for these programs. G&T also coordinates with other relevant parts of the DHS family to bring their subject matter expertise to bear on specific grants and initiatives.

DHS is committed to working with the owners and operators of America's critical infrastructure as part of the national effort to reduce the risks from terrorism and other threats to the homeland.



Michael Chertoff
Secretary
Department of Homeland Security

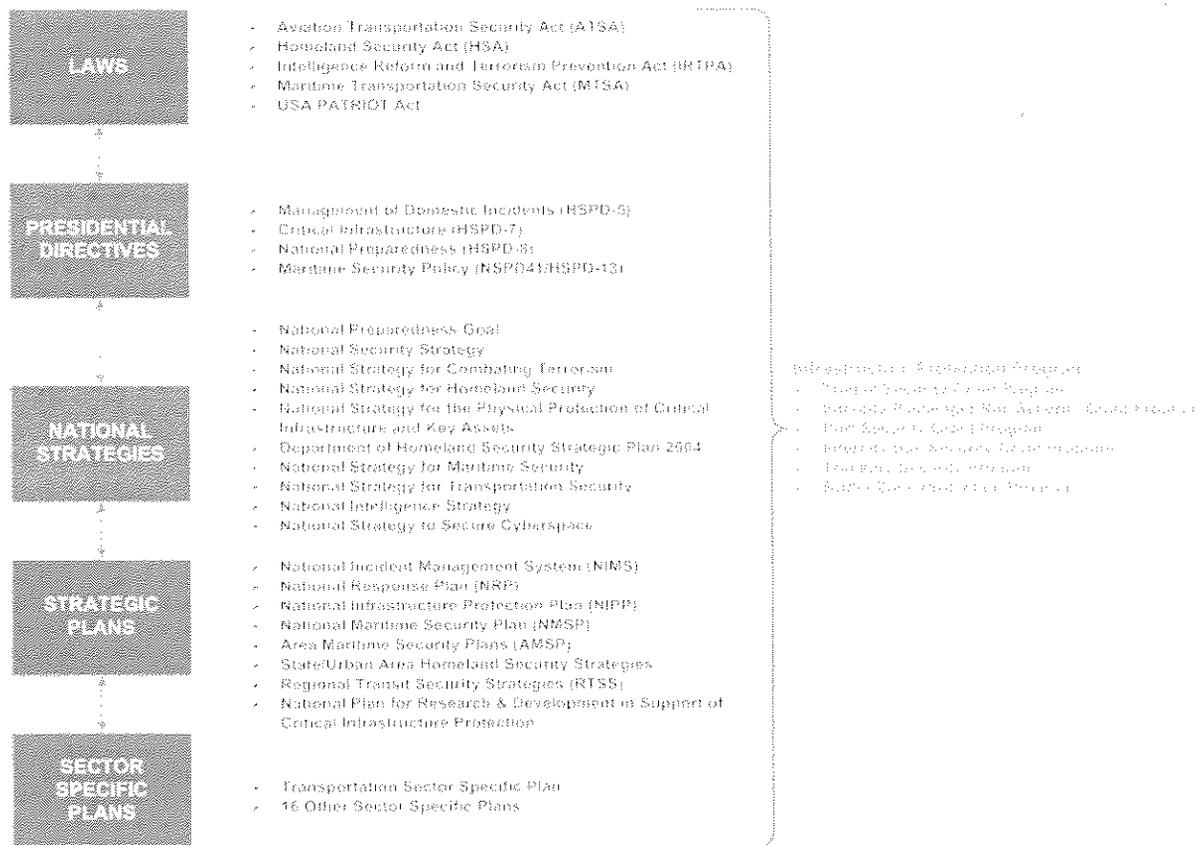
Contents

Part I	Introduction	1
Part II	FY 2006 Port Security Grant Program	2
Part III	Eligible Applicants and Funding Availability	7
Part IV	Program and Application Requirements	11
Part V	Assistance Resources and Support	21
Part VI	Reporting, Monitoring and Closeout Requirements	23
Appendix A	Authorized Program Expenditures Guidance	
Appendix B	Port System Overview Template Guidance	
Appendix C	Individual Project Plan Template Guidance	
Appendix D	Budget Detail Worksheet Guidance	
Appendix E	MOU/MOA Guidance	
Appendix F	Canine Acquisition Start-up Costs Certification Guidance	
Appendix G	Captain of the Port Zone Abbreviations	
Appendix H	Application Checklist	
Appendix I	Grants.Gov Quick Start Instructions	
Appendix J	Post Award Instructions	
Appendix K	Additional Guidance on the National Preparedness Goal and the National Priorities	
Appendix L	Capabilities Based Planning Guidance	
Appendix M	National Incident Management System Guidance	
Appendix N	National Infrastructure Protection Plan Guidance	
Appendix O	Public Safety Communications and Interoperability Guidance	
Appendix P	Domestic Nuclear Detection Office Guidance	
Appendix Q	National Environmental Policy Act Guidance	
Appendix R	Acronyms and Abbreviations	

I. Introduction

The FY 2006 Port Security Grant Program (PSGP) is an important component of the Administration's larger, coordinated effort to strengthen the security of America's critical infrastructure. This program implements the objectives addressed in a series of laws, strategy documents, plans and Homeland Security Presidential Directives (HSPDs) outlined in Figure 1. Of particular significance are the National Preparedness Goal (the Goal)* and its associated work products, the National Infrastructure Protection Plan (NIPP)* and the National Strategy for Transportation Security (NSTS).

Figure 1. Laws, Strategy Documents, Directives and Plans That Impact the Infrastructure Protection Program



On March 31, 2005, DHS issued the Interim National Preparedness Goal. The Goal establishes a vision for a National Preparedness System. A number of the key building blocks for that system, including the National Planning Scenarios, Universal Task List (UTL), Target Capabilities List (TCL), and the seven National Priorities are important components of a successful Port Security Grant.

* As this grant guidance went to print, the final Goal and the NIPP are being prepared for release.

II. The FY 2006 Port Security Grant Program

The mission of the FY 2006 Port Security Grant Program is to create a sustainable, risk-based effort for the protection of critical port infrastructure from terrorism, especially explosives and non-conventional threats that would cause major disruption to commerce and significant loss of life.

A. Program Overview

As a component of the Infrastructure Protection Program (IPP), the FY 2006 PSGP seeks to assist the Nation's ports in obtaining the resources and capabilities required to support the National Preparedness Goal and the associated National Priorities. Through its focus on port-wide risk management planning, improvised explosive devices, non-conventional methods of attack and domain awareness in the port environment, the FY 2006 PSGP directly addresses six of the seven National Priorities:

- 1) expanding regional collaboration;
- 2) implementing the National Incident Management System and the National Response Plan;
- 3) implementing the National Infrastructure Protection Plan;
- 4) strengthening information sharing and collaboration capabilities;
- 5) enhancing interoperable communications capabilities; and,
- 6) strengthening CBRNE detection and response capabilities.

In addition, the FY 2006 PSGP also supports strengthening emergency operations planning and citizen protection capabilities, and assists in addressing security priorities specific to the port environment.

B. Solicitation Overview

The FY 2006 Port Security Grant Program is the sixth round of grants and builds upon the previous five (5) rounds. ***Successful applications will be selected by a competitive process. Following risk-based national port security priorities, the FY 2006 PSGP will place a strong emphasis on prevention and detection against improvised explosive devices (IEDs). Of great concern are IEDs delivered via small craft, underwater and in vehicles on ferries. In addition, projects that demonstrate enhanced Maritime Domain Awareness (e.g., access control/standardized credentialing, command and control, communications and enhanced intelligence sharing and analysis) will also receive preference under the FY 2006 PSGP.***¹

¹ The national priorities are consistent with HSPD-13 (December 21, 2005), which established as maritime security policies: "preventing terrorist attacks or criminal acts or hostile acts in, or the unlawful exploitation of, the Maritime Domain, and reducing the vulnerability of the Maritime Domain to such acts and exploitation" and "enhancing U.S. national security and homeland security by protecting U.S. population centers, critical infrastructure, borders, harbors, ports and coastal approaches in the Maritime Domain." Prevention of terrorist attacks and criminal or hostile acts and protection of maritime related population centers and critical infrastructure were incorporated as strategic objectives within *The National Strategy for Maritime Security* (September 2005).

Eligible applicants in each port area may submit one application for funding of up to five (5) individual projects.² Funding may be awarded for all, some or none of the projects submitted based on the outcome of the evaluation process.

G&T will coordinate and participate in a Federal interagency application review with USCG, Office of Infrastructure Protection (OIP), the Transportation Security Agency (TSA), and Customs and Border Protection (CBP) within DHS, and Maritime Administration (MARAD) within the Department of Transportation.

C. Project Selection

As noted in Section B above, a series of reviews will occur among local and national subject matter experts to ensure the most effective distribution of funding among these ports. Awards under this program will not be based on formula distributions, but rather on risk-based analytical assessments that align with the national goals outlined in this grant application package.

1. **Initial Screening.** G&T staff will receive and conduct an initial review of all FY 2006 PSGP applications. Submitters are responsible for ensuring that ineligible, incomplete and duplicate applications are not submitted – doing so may cause elimination from further consideration. Applications passing this review will be grouped by port area and provided to the applicable Captain of The Port (COTP) for further review.
2. **Field Review.** Field level reviews will be managed by the applicable COTP in coordination with the MARAD Region Director and appropriate personnel from the Area Maritime Security Committee (AMSC) and/or local law enforcement (as identified by the COTP). To support coordination of security grant application projects with state and urban area homeland security strategies, as well as other State and local security plans, the COTP will coordinate the results of the field review with the applicable State Administrative Agency or Agencies and the State Homeland Security Advisors. For each port, the COTP will submit to DHS evaluations that include the following: (1) each specific application will be scored for compliance with the four core grant program criteria enumerated below, and a total score will be computed; and (2) all proposals received from each port will be rank ordered from highest to lowest in terms of their contributions to risk reduction and cost effectiveness. The four core PSGP criteria are as follows:
 - *Criteria #1.* Projects that support the national port security priorities:
 - Prevention and detection of IED attacks by small craft;

² An individual project could be a single activity or multiple activities required to complete an action, such as the establishment of a canine program or an enhanced employee identification system. Individual projects must take place at a single port area.

- Prevention and detection of vehicle-borne IEDs on ferries;
- Prevention and detection of underwater IED attacks; and,
- Enhancement of the port area's Maritime Domain Awareness (e.g., access control/standardized credentialing, command and control, communications and enhanced intelligence sharing and analysis);
- *Criteria #2.* Projects that address priorities outlined in the applicable Area Maritime Security Plan (AMSP - mandated under the Maritime Transportation Security Act (MTSA));
- *Criteria #3.* Projects that address additional security priorities based on the COTP's expertise and experience with the specific port area; and,
- *Criteria #4.* Projects that offer the highest potential for risk reduction for the least cost.

Projects will be rated against the above noted program criteria. The COTP will score specific applications on a four-point scale, and scores will reflect responsiveness to the four core criteria. To assist submitters in preparing their applications, the scoring scale to be used in gauging the application and its specific components are outlined below.

Figure 2. Field Review Scoring of Responsiveness to Core Program Criteria

Rating Criteria:

- **Criteria #1** will be scored on a scale of 0 to 4, as follows:
 - 0 = Not applicable, project does not address one of the National Priorities
 - 1 = Project will be marginally effective in preventing/detecting the threat
 - 2 = Project will be moderately effective in preventing/detecting the threat
 - 3 = Project will be very effective in preventing/detecting the threat
 - 4 = Project will be extremely effective in preventing/deterring the threat
- **Criteria #2** will be scored on a scale of 0 to 4, as follows:
 - 0 = Project is not responsive to the AMSP
 - 1 = Project is marginally responsive to the AMSP
 - 2 = Project is moderately responsive to the AMSP
 - 3 = Project is very responsive to the AMSP
 - 4 = Project is extremely responsive to the AMSP
- **Criteria #3** will be scored on a scale of 0 to 4, as follows:
 - 0 = Project will not impact additional security priorities
 - 1 = Project will have a marginal impact on additional security priorities
 - 2 = Project will have a moderate impact on additional security priorities
 - 3 = Project will have a substantial impact on additional security priorities
 - 4 = Project will have a major impact on additional security priorities
- **Criteria #4** will be scored on a scale of 0 to 4, as follows:
 - 0 = Project offers no risk reduction potential for the cost
 - 1 = Project offers marginal risk reduction potential for the cost
 - 2 = Project offers moderate risk reduction potential for the cost
 - 3 = Project offers good risk reduction potential for the cost
 - 4 = Project offers outstanding risk reduction potential for the cost

After completing field reviews, the COTPs will submit prioritized listings of projects for each port area to USCG District staff to ensure consistent application of field review guidance. After review by USCG District staff, COTPs will then submit the field review prioritized lists to G&T to begin coordination of the national review process.

3. **National Review.** Following the field review, a National Review Panel will be convened. The panel will include subject matter experts from G&T, USCG, TSA, CBP, OIP and MARAD. The purpose of the National Review Process is to identify a final, prioritized list of projects for funding.

The National Review Panel will conduct an initial review of the prioritized project listings for each port area submitted by the USCG COTP to ensure that the proposed projects will accomplish intended risk mitigation goals. The National Review Panel will validate the Field Review COTP Project Priority List and provide a master list of prioritized projects by port area. Following this initial meeting, G&T will review the projects from the National Review Panel's validated prioritized list for each port area against a risk-based algorithm that considers the following factors to produce a comprehensive national priority ranking of port security proposals.

- Relationship of the project to one or more of the national port security priorities:
- The relationship of the project to one or more of the local port security priorities:
- The COTP's ranking (based on each COTP's prioritized list of projects); and,
- The location of the project based on DHS's risk assessment ranking of U.S. Ports.
- The relationship of the project to one or more of the National Priorities outlined in the National Preparedness Goal.

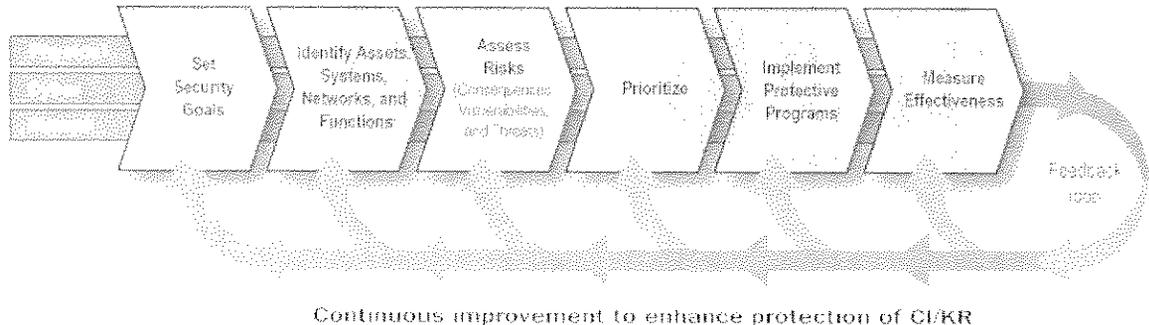
In order to assure that port areas are competing for funds on an equal footing with port areas with similar risk ratings, each port area will be sorted by risk into tiers. Each tier will be given a specific allotment of grant funds for which port areas will compete. ***Consequently, applicants will compete for funding against only those port areas with similar risk rankings.***

The National Review Panel will then be asked to evaluate and validate the consolidated and ranked project list resulting from this process. Past performance on previous Port Security Grant Program awards may be taken into consideration in reviewing the ranked project list. Awards will be made based on the final ranked list of projects identified by the National Review Panel. ***After DHS final approval, a final listing of awards for each port area will be provided to the awardee and to the relevant COTP, MARAD Region Director, AMSC, State Administrative Agency(ies) and Homeland Security Advisor(s).***

D. The Goal, Risk Management and Planning Requirements Associated with the FY 2006 Port Security Grant Program

During FY 2006 the Preparedness Directorate, working jointly with the USCG, will continue their work to enhance the risk-based allocation of funds developed in FY 2005, to coordinate port security planning efforts, such as the Area Maritime Security Plan with other risk management planning strategies that have been developed by State and Urban areas. This process will be the beginning of a fundamental shift in the focus of the Port Security Grant Program from primarily a facility security focused grant program to a Port-Wide Risk Management program as part of urban area and state efforts. As such, this process will embody in the development of an integrated risk-based decision making process for each port area. The process will be patterned after the Risk Management Framework articulated in the National Infrastructure Protection Plan. (see Figure 3) Adoption of a deliberate risk management planning process will enable the Federal Maritime Security Coordinator (FMSC) and AMSC to make security enhancement decisions in the context of strategic security goals, supported by clear, measurable objectives. This process will also allow port area security needs to be integrated into the broader national risk management framework of the National Infrastructure Protection Plan, regional planning construct that forms the core of the UASI program, as well as, statewide initiatives.

Figure 3. NIPP Framework



III. Eligible Applicants and Funding Availability

A. Eligible Applicants

The FY 2006 DHS Appropriations Act provides funds for a competitive grant program to address physical security enhancements for critical national seaports. DHS has expanded the eligibility to apply for funding in FY 2006. However, it is important to note that risk-based distribution of funding remains a high priority for the PSGP. *DHS, through G&T, will award the available funds to projects offering the greatest risk reduction potential in the Nation's highest risk port areas, thereby ensuring federally regulated ports, terminals and U.S. inspected passenger vessels receiving the funds represent assets of the highest strategic importance nationally.*

One hundred seaports³, representing 95 percent of the foreign waterborne commerce of the United States, plus an additional port area eligible in FY 2005, have been identified for inclusion in the FY 2006 PSGP. Eligible facilities within these port areas must be within two miles of the commercial waterway. Additionally, if a facility falls outside the recognized boundaries of one of these port areas, but is addressed in the port's AMSP, it will be considered eligible.

Table 1 below identifies the port areas in which grant activity may take place. However, please note that *presence on this list does not guarantee receipt of grant funding.* The port areas are listed alphabetically – no additional significance should be attributed to this ordering.

Table 1. Port Areas Eligible for Consideration of Funding

FY 2006 PSGP Eligible Port Areas	
Albany, NY	Nashville, TN
Anacortes, WA	New Haven, CT
Anchorage, AK	New London, CT
Baltimore, MD	New Orleans, LA
Baton Rouge, LA	New York/New Jersey
Beaumont, TX	Newport News, VA
Boston, MA	Norfolk Harbor, VA
Bridgeport, CT	Oakland, CA
Brownsville, TX	Palm Beach, FL
Buffalo, NY	Panama City, FL
Burns Harbor, IN	Pascagoula, MS
Camden, NJ	Paulsboro, NJ
Charleston, SC	Penn Manor, PA
Chattanooga, TN	Pensacola, FL

³ This eligibility list was developed by the U.S. Coast Guard using commercial, demographic and geographic data from various sources. Factors such as Cargo Volume and Passenger Volume, the presence of Critical Infrastructure/Key Assets (CI/KA), and Strategic Importance, among others, were utilized in the determination. Its purpose is to identify ports that are essential to the viability of the Marine Transportation System. Ports on this list represent 95 percent of the foreign waterborne commerce of the United States. Use of this list for other purposes may not be warranted.

Chester, PA	Philadelphia, PA
Chicago, IL	Pittsburgh, PA
Cincinnati, OH	Plaquemines, LA
Cleveland, OH	Ponce, PR
Corpus Christi, TX	Port Arthur, TX
Detroit, MI	Port Canaveral, FL
Duluth-Superior, MN/WI	Port Everglades, FL
Everett, WA	Port Hueneme, CA
Freeport, TX	Port Manatee, FL
Galveston, TX	Port St. Joe, FL
Gary, IN	Portland, ME
Green Bay, WI	Portland, OR
Greenville, MS	Portsmouth, NH
Gulfport, MS	Providence, RI
Guntersville, AL	Richmond, CA
Helena, AR	San Diego, CA
Honolulu, HI	San Francisco, CA
Houston, TX	San Juan, PR
Huntington, WV	Savannah, GA
Indiana Harbor, IN	Seattle, WA
Jacksonville, FL	South Louisiana, LA
Kalama, WA	St. Louis, MO
Kansas City, MO	St. Paul, MN
Lake Charles, LA	Stockton, CA
Long Beach, CA	Tacoma, WA
Longview, WA	Tampa, FL
Los Angeles, CA	Texas City, TX
Louisville, KY	Toledo, OH
Marcus Hook, NJ	Tulsa, OK
Matagorda, TX	Two Harbors, MN
Memphis, TN	Valdez, AK
Miami, FL	Vancouver, WA
Milwaukee, WI	Vicksburg, MS
Minneapolis, MN	Victoria, TX
Mobile, AL	Wilmington, DE
Morehead City, NC	Wilmington, NC
Mount Vernon, IN	

New Port Areas Eligible for FY 2006 PSGP

Within the eligible port areas, applicants must be:

- Owners/operators of federally regulated ports, terminals, facilities, U.S. inspected passenger vessels, or ferries as defined in the Maritime Transportation Security Act (MTSA) 33 CFR Parts 101, 104, and 105;
- Port authorities or other state and local agencies that provide layered security protection to federally regulated facilities in accordance with an AMSP or a facility or vessel security plan; or,
- Consortia composed of local stakeholder groups (e.g., river groups, ports, and terminal associations) representing federally regulated ports, terminals, U.S.

inspected passenger vessels, or ferries that provide layered security protection to federally regulated facilities in accordance with an AMSP or a facility or vessel security plan.

For purposes of the FY 2006 PSGP, layered security means an approach that utilizes prevention and detection capabilities of organizations within a port-wide area to provide complete security solutions to regulated entities. For example, organizations can provide layered protection through command and control functions, waterside measures that address security over multiple terminals and facilities or U.S. inspected passenger vessel operations (as defined under CFR Part 104) within a port area.

There are three recognized kinds of organizations that provide port-wide layered security: a port authority, state and local governments, and consortia or associations which represent MTSA regulated entities as defined in 33 CFR Parts 101, 104, and 105.

- A port authority may provide layered security through port-wide prevention and detection activities on behalf of all port users, the landlord for the tenants on port property, or as the owner operator of the port operations. This layered security must include MTSA regulated entities and the layered security provided by the port authority must be addressed in the regulated entities' security plans.
- State and local governments, through law enforcement or other recognizable state or local agencies, may also provide layered security for MTSA regulated entities. Those government agencies that are responsible for maintaining security for MTSA regulated entities must be addressed in the regulated entities' security plan or in the AMSP developed by the USCG COTP and the AMSC.
- Consortia or associations that provide layered security to MTSA regulated facilities. In addition, the layered protection provided must be addressed in the regulated entities' security plans.

Ownership of port facilities varies from port to port. In some cases, individual tenants own land within a port, while others lease their space from the port entity. Additionally, approximately 90 percent of the Nation's port infrastructure is privately owned and operated. Within ports, the highest risk assets include oil, chemical, gas terminals and passenger/ferry vessels/terminals that are often owned/operated by the private sector. The Department recognizes the unique challenges this represents with respect to port-wide risk reduction. The Department also believes that security should be a shared responsibility.

B. Funding Availability

The FY 2006 PSGP will provide \$168,052,500 for port security grants. Funding will be provided directly to successful applicants.

IV. Program and Application Requirements

A. General Program Requirements

Successful applicants will be responsible for administration of FY 2006 PSGP awards. In administering the program, the applicant must comply with the following requirements.

1. **Matching Funds.** Consistent with FY06 Congressional appropriation requirements, **Public Sector** applicants must provide matching funds supporting at least **25 percent of the total project cost** for each proposed project. As with the FY05 grant requirements, **Private Sector** applicants must provide matching funds supporting at least **50 percent of the total project cost** for each proposed project.

Exceptions: There is no matching requirement for projects with a total cost less than \$25,000. If the Secretary of Homeland Security determines that a proposed project merits support and cannot be undertaken without a higher rate of Federal support, the Secretary may approve grants with a matching requirement other than that specified in accordance with 46 USC Sec. 70107(c)(2)(B).

2. **Management and Administration Costs.** Any management and administration (M&A) costs associated with individual projects submitted for consideration of funding under the FY 2006 PSGP must be included in the budget for that project. M&A costs associated with managing the overall PSGP award itself must be accounted for separately from program costs in the detailed budget. **M&A costs may not exceed three (3) percent of the total grant award.**

B. Specific Program Requirements

1. **National Port Security Priorities.** When developing project proposals for the FY 2006 PSGP, specific attention should be paid to prevention and detection of attacks involving IEDs. IEDs pose a threat of great concern to transportation systems across the nation. IEDs have historically been a terrorist weapon of choice because they combine a high degree of effectiveness with minimal cost. *Of great concern to port security are IEDs delivered via small craft, underwater and including vehicles on ferries. Particular areas of focus, therefore, should include: protection of facilities (including commercial port facilities, public cruise line and ferry terminals) and vessels from tampering and attack. Additionally, priority will be given to projects that enhance the port system's Maritime Domain Awareness (i.e. access control/standardized credentialing, command and control, communications and enhanced intelligence sharing and analysis).*

C. Ineligible Activities/Costs

The following projects and costs are considered ineligible for award consideration:

- Ferry systems participating in the FY 2006 Transit Security Grant Program (TSGP) cannot apply for funding for projects already under consideration for other TSGP funding;
- The development of risk/vulnerability assessment models and methodologies;
- Projects in which Federal agencies are the primary beneficiary or that enhance Federal property;
- Projects that study technology development for security of national or international cargo supply chains (e.g., e-seals, smart containers, container tracking, container intrusion detection devices);
- Proof-of-concept projects;
- Projects involving training and exercises that do **not** meet MTSA standards and/or requirements set by MTSA or the DHS Preparedness Directorate;
- Projects that do not provide a compelling security benefit (e.g., primarily economic or safety vs. security);
- Projects that duplicate capabilities being provided by the Federal government (e.g., vessel traffic systems, etc.);
- Proposals in which there are real or apparent conflicts of interest;
- Personnel costs (except for direct management and administration of the grant awards, (i.e., preparation of mandatory post-award reports);
- Business operating expenses (Certain security-related operational and maintenance costs are allowable. See "Specific Guidance on Security Operational and Maintenance Costs" in Appendix A (Sec F) for further guidance);
- Reimbursement of pre-award security expenses;
- Repair of existing equipment including, but not limited to: fencing, lighting, CCTV, access controls, etc.;
- Weapons, including, but not limited to: firearms and ammunition, for outfitting facilities, vessels, or other structures; and,
- Outfitting facilities, vessels, or other structures with equipment or items providing a hospitality benefit rather than a direct security benefit. Examples of such equipment or items include, but are not limited to: office furniture, CD players, DVD players, AM/FM radios, etc.

D. Application Requirements

The following steps must be completed using the on-line <http://www.grants.gov> system to ensure a successful application submission:

1. Application Process

DHS is participating in the e-Government initiative, one of 25 initiatives included in the President's Management Agenda (PMA). Grants.gov, part of the PMA, is a "storefront" that provides a unified process for all customers of Federal grants to find funding opportunities and apply for funding. **Applicants must apply for FY 2006 PSGP funding through Grants.gov at <http://www.grants.gov>. Complete**

applications must be received by G&T no later than 11:59 pm EST on August 4, 2006.

2. On-Line Application

The on-line application must be completed and submitted by an authorized representative of the applicant organization using Grants.gov. The on-line application replaces the following previously required paper forms:

- Standard Form 424, Application for Federal Assistance;
- Standard Form LLL, Disclosure of Lobbying Activities;
- JP Form 4000/3, Assurances;
- JP form 4061/6, Certifications; and,
- Non-Supplanting Certification.

The program title listed in the Catalog of Federal Domestic Assistance (CFDA) is "Port Security Grant Program." The CFDA number is 97.056. When completing the on-line application, applicants should identify their submissions as new, non-construction applications. *It is important to note that this is a procedural requirement within Grants.gov and does not prohibit the applicant from submitting construction projects.* The project period will be for a period not to exceed 30 months.

3. Application Submission Requirements

Eligible applicants may submit one application for funding of up to five (5) individual projects. The individual projects comprising a single application must take place within the same port area. Private companies that operate in more than one eligible port area must submit separate applications for projects in each port area. Applicants will be given an opportunity to make changes to their application until the close of the application period. It is important to note, however, that simple clerical errors in the application submissions will NOT render an application ineligible.

As part of the application process, the applicant must include a Port System Overview. Applicants must also provide a project plan and detailed budget for each proposed project.

Applicants should use the following file name conventions for files attached in Grants.gov:

COTP __ Port Area__ Name of Applicant__ Document Type__ Project Number

Example #1: PWS_Valdez_State Ferry System_Port System Overview

Example #2: PWS_Valdez_State Ferry System_Project Plan_Project1

Example #3: PWS_Valdez_State Ferry System_Project Budget_Project1

Example #4: PWS_Valdez_State Ferry System_Program Budget_M&A Costs

➤ **Port System Overview** – Each Port System Overview, provided by the applicant, should not exceed ten (10) pages. The Port System Overview should identify specific point(s) of contact (POC) to work with DHS on the implementation of the FY 2006 PSGP. As part of the application process, applicants must provide data/statistics that relate to their specific port project (for port applications), terminal project (for terminal applications), waterways, and U.S. inspected passenger vessel or ferry projects. Terminals and vessels cannot rely on aggregated port statistics. The Port System Overview should include the following information:

- Area of Operations (including COTP Zone and eligible port as identified in Table 1);
- POC(s) for Organization;
- Ownership/operation (identification of the applicant as a publicly or privately owned facility, public entity, consortium or association, etc.);
- Role in Layered Protection of Regulated Entities (if applicable);
- Infrastructure;
- Current IED capabilities;
- Domain Awareness Capabilities;
- Nature of Operations, including:
 - Type and Volume of Cargo (annual statistics); and, if applicable,
 - Type and Volume of Hazardous Materials (annual statistics); and, if applicable,
 - Number of Passengers (annual statistics); and, if applicable,
 - Number of Vessels Owned;
- Any other important features; and,
- Brief summary of security enhancements already undertaken (including those supported through previous Federal grant awards).

In addition, the Port System Overview should address the applicant's current IED prevention and detection capabilities, as well as its domain awareness capacities (i.e., command, control, communications, and enhanced intelligence sharing and analysis). Applicants that submit more than one project must also provide a listing of these projects in order of priority, and a justification for the prioritization.⁴

⁴ **Prevention:** Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions taken to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and

- **Individual Project Plan** – Applications must clearly demonstrate an ability to provide tangible, physical security enhancements consistent with the purpose of the program and guidance provided by DHS. The applicant must provide a complete project plan for the entire project period. The project plan must demonstrate how the project would address a vulnerability identified in the applicant's USCG approved security plan. The Project Plan should demonstrate how the project addresses the National Priorities of the National Preparedness Goal (i.e., implementing the National Infrastructure Protection Plan, Regionalism, Implementing the National Incident Management System, and Achieving interoperable communications). The project plan must also clearly demonstrate how the project is consistent with all applicable requirements outlined in this application kit and addresses the rating criteria identified in *Section II: The FY 2006 Port Security Grant Program*. The project period will be for a period not to exceed **30 months**. Each project plan should not exceed five (5) pages. ***Applications must include a separate Individual Project Plan for each proposed project.***

- **Detailed Budget** – The applicant must also provide a detailed budget for use of the funds requested (see Appendix A for guidance on allowable costs under this program). The budget must be complete, reasonable and cost-effective in relation to the proposed project. The budget should provide the basis of computation of all project-related costs, including any appropriate narrative. The budget should also demonstrate any cash match. Public sector applicants must provide matching funds supporting **at least 25 percent of the total project cost** for each proposed project. Private sector applicants must provide matching funds supporting **at least 50 percent of the total project cost** for each proposed budget. ***Applications must include a separate budget for each proposed project.***

Important Note: If an applicant determines that a higher level of (Federal) support is required for a project, the applicant must demonstrate the "merits" of the project within the Budget Narrative for review by the Secretary and or appropriate designee in accordance with 46 USC Sec. 70107(c)(2)(B) for a waiver to the match requirement to be considered.

source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice. (Source—National Incident Management System, March 2004)

4. National Environmental Policy Act (NEPA)

NEPA requires DHS, through G&T, to analyze the possible environmental impacts of each construction project. The purpose of a NEPA review is to weigh the impact of major Federal actions or actions undertaken using Federal funds on adjacent communities, water supplies, historical buildings, endangered species, or culturally sensitive areas prior to construction. Grantees wishing to use DHS funding for construction projects must complete and submit a NEPA Compliance Checklist to DHS for review. Additionally, grantees may be required to provide additional detailed information on the activities to be conducted, locations, sites, possible construction activities, possible alternatives, and any environmental concerns that may exist. Results of the NEPA Compliance Review could result in a project not being approved for DHS funding, the need to perform an Environmental Assessment (EA) or draft an Environmental Impact Statement (EIS).

[Redacted area]

5. MOU/MOA Requirement for State or Local Agencies and for Consortia or Associations

State and local agencies, as well as consortia or associations (as defined in *Section III: Eligible Applicants and Funding Availability*) which provide layered security to MTSA regulated facilities are eligible applicants. However, the layered protection provided must be addressed in the regulated entities' security plans. A copy of an MOU/MOA with the identified regulated entities will be required prior to funding, and must include an acknowledgement of the layered security and roles and responsibility of all entities involved. ***Eligible public port authorities, or other state or local agencies and consortia or associations must provide this information. This information may be provided using one of the attachment fields within Grants.gov.***

[Redacted area]

6. Universal Identifier

The applicant must provide a Dun and Bradstreet (D&B) Data Universal Numbering System (DUNS) number with the application. An application will not be considered complete until a valid DUNS number is provided by the applicant. This number is a required field within Grants.gov. Organizations should verify that they have a DUNS number or take the steps necessary to obtain one as soon as possible.

7. Compliance with Federal Civil Rights Laws and Regulations

Grantees are required to comply with Federal civil rights laws and regulations. Specifically, grantees are required to provide assurances as a condition for receipt of Federal funds from DHS that its programs and activities comply with the following:

- *Title VI of the Civil Rights Act of 1964, as amended, 42 USC 2000 et. seq.* – no person on the grounds of race, color or national origin will be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination in any program or activity receiving Federal financial assistance;
- *Section 504 of the Rehabilitation Act of 1973, as amended, 29 USC 794* – no qualified individual with a disability in the United States, shall, by reason of his or her disability, be excluded from the participation in, be denied the benefits of, or otherwise be subjected to discrimination in any program or activity receiving Federal financial assistance;
- *Title IX of the Education Amendments of 1972, as amended, 20 USC 1681 et. seq.* – discrimination on the basis of sex is eliminated in any education program or activity receiving Federal financial assistance; and,
- *The Age Discrimination Act of 1975, as amended, 20 USC 6101 et. seq.* – no person in the United States shall be, on the basis of age, excluded from participation in, denied the benefits of or subjected to discrimination under any program or activity receiving Federal financial assistance.

Grantees must comply with all regulations, guidelines, and standards adopted under the above statutes. Grantees are also required to submit information, as required, to the DHS Office for Civil Rights and Civil Liberties concerning its compliance with these laws and their implementing regulations.

8. Financial Requirements

- **Non-Supplanting Certification:** This certification affirms that these grant funds will be used to supplement existing funds and will not replace (i.e., supplant) funds that have been appropriated for the same purpose. Potential supplanting will be addressed in the application review as well as in the pre-award review, post-award monitoring and any potential audits. Applicants or grantees may be required to supply documentation certifying that a reduction in non-Federal resources occurred for reasons other than the receipt or expected receipt of Federal funds.
- **Match Requirement:** Public sector applicants must provide matching funds supporting **at least 25 percent of the total project cost** for each proposed project. Private sector applicants must provide matching funds supporting **at least 50 percent of the total project cost** for each proposed project.

Exceptions: There is no matching requirement for projects with a total cost that does not exceed more than \$25,000. If the Secretary determines that a proposed project merits support and cannot be undertaken without a higher rate of Federal support, the Secretary may approve grants with a matching requirement other than that specified in accordance with 46 USC Sec. 70107(c)(2)(B). For further information defining match, timing of match contributions and records for match, please consult the Office of Grant Operations (OGO) *Financial Management Guide*, available at <http://www.dhs.gov/dhsaupboidisplay?bopid=16>.

- **Accounting System and Financial Capability Questionnaire:** All nongovernmental (non-profit and commercial) organizations that apply for funding with DHS that have not previously (or within the last 3 years) received funding from DHS must complete the Accounting System and Financial Capability Questionnaire. *This information may be provided using one of the attachment fields within the on-line Grants.gov application.*

<http://www.oip.usdoj.gov/oc>

- **Assurances:** Assurances forms (SF-424B and SF-424D) can be accessed at <http://apply.grants.gov/agency/FormLinks?family=7>. It is the responsibility of the recipient of the Federal funds to fully understand and comply with these requirements. Failure to comply may result in the withholding of funds, termination of the award, or other sanctions. The applicant will be agreeing to these assurances upon the submission of the application.
- **Certifications Regarding Lobbying; Debarment, Suspension, and Other Responsibility Matters; and Drug-Free Workplace Requirement:** This certification, which is a required component of the on-line application, commits the applicant to compliance with the certification requirements under 28 CFR part 67, *Government-wide Debarment and Suspension (Non-procurement)*; 28 CFR part 69, *New Restrictions on Lobbying*; and 28 CFR part 83 *Government-wide Requirements for Drug-Free Workplace (Grants)*. All of these can be referenced at: http://www.access.gpo.gov/nara/cfr/waisidx_04/28cfrv2_04.html.

The certification will be treated as a material representation of the fact upon which reliance will be placed by DHS in awarding grants.⁶

9. Services to Limited English Proficient (LEP) Persons

Recipients of DHS financial assistance are required to comply with several Federal civil rights laws, including Title VI of the Civil Rights Act of 1964, as amended. These laws prohibit discrimination on the basis of race, color, religion, national origin, and sex in the delivery of services. National origin discrimination includes discrimination on the basis of limited English proficiency. To ensure compliance with

Title VI, recipients are required to take reasonable steps to ensure that LEP persons have meaningful access to their programs. Meaningful access may entail providing language assistance services, including oral and written translation, where necessary. Grantees are encouraged to consider the need for language services for LEP persons served or encountered both in developing their proposals and budgets and in conducting their programs and activities. Reasonable costs associated with providing meaningful access for LEP individuals are considered allowable program costs. For additional information, please see <http://www.dhs.gov>.

10. Integrating Individuals with Disabilities into Emergency Planning

Executive Order #13347, entitled "Individuals with Disabilities in Emergency Preparedness" and signed in July 2004, requires the Federal government to support safety and security for individuals with disabilities in situations involving disasters, including earthquakes, tornadoes, fires, floods, hurricanes, and acts of terrorism. Consequently, Federal agencies are required to: 1) encourage consideration of the unique needs of persons with disabilities in emergency preparedness planning; and 2) facilitate cooperation among Federal, state, local, and tribal governments, private organizations, non-governmental organizations, and the general public in the implementation of emergency preparedness plans as they relate to individuals with disabilities. A January 2005 letter to state governors from then-Homeland Security Secretary Tom Ridge asked states to consider several steps in protecting individuals with disabilities:

- Ensure that existing emergency preparedness plans are as comprehensive as possible with regard to the issues facing individuals with disabilities;
- Ensure that emergency information and resources are available by accessible means and in accessible formats; and,
- Consider expending Federal homeland security dollars on initiatives that address and/or respond to the needs of individuals with disabilities for emergency preparedness, response, and recovery.

Further information can be found at the Disability and Emergency Preparedness Resource Center at <http://www.dhs.gov/e-s/dhs/preparedness>. This resource center provides information to assist emergency managers in planning and response efforts related to people with disabilities. In addition, all grantees should be mindful of Section 504 of the Rehabilitation Act of 1973 that prohibits discrimination based on disability by recipients of Federal financial assistance.

11. Freedom of Information Act (FOIA)

DHS recognizes that much of the information submitted in the course of applying for funding under this program, or provided in the course of its grant management activities, may be considered law enforcement sensitive or otherwise important to national security interests. This may include threat, risk, and needs assessment information discussions of demographics, transportation, public works, industrial

and public health infrastructures. While this information under Federal control is subject to requests made pursuant to the FOIA, 5. USC §552, all determinations concerning the release of information of this nature are made on a case-by-case basis by the DHS FOIA Office, and may likely fall within one or more of the available exemptions under the Act. Applicants are encouraged to consult their own state and local laws and regulations regarding the release of information, which should be considered when reporting sensitive matters in the grant application, needs assessment and strategic planning process. Applicants may also consult their G&T Program Manager regarding concerns or questions about the release of information under state and local laws. Grantees should be familiar with the regulations governing Protected Critical Infrastructure Information (6 CFR Part 29) and Sensitive Security Information (49 CFR Part 1520), as these designations may provide additional protection to certain classes of homeland security information.

12. Geospatial Guidance

Geospatial technologies capture, store, analyze, transmit, and/or display location-based information (i.e., information that can be linked to a latitude and longitude). In geospatial systems, this location information is often paired with detailed information about the location such as: purpose/use, status, capacity, engineering schematics, operational characteristics, environmental and situational awareness. State and local emergency organizations are increasingly incorporating geospatial technologies and data to prevent, protect against, respond to, and recover from terrorist activity and incidents of national significance. In the preparedness phase, homeland security planners and responders need current, accurate, and easily accessible information to ensure the readiness of teams to respond. Also an important component in strategy development is the mapping and analysis of critical infrastructure vulnerabilities, and public health surveillance capabilities. Geospatial information can provide a means to prevent terrorist activity by detecting and analyzing patterns of threats and possible attacks, and sharing that intelligence. During response and recovery, geospatial information is used to provide a dynamic common operating picture, coordinated and track emergency assets, enhance 911 capabilities, understand event impacts, accurately estimate damage, locate safety zones for quarantine or detention, and facilitate recovery. Use of Federal homeland security dollars for geospatial activities requires pre-approval and a demonstrated capability for robust interoperability with DHS and other relevant systems. G&T will coordinate review of requests for use of Federal homeland security funding for other geospatial projects with relevant entities.

V. Assistance Resources and Support

A. Drawdown and Expenditure of Funds

G&T's Office of Grant Operations (OGO) will provide fiscal support of the grant programs included in this solicitation, with the exception of payment related issues. For financial and administrative questions, all grant and sub grant recipients should refer to the OGO *Financial Management Guide* or contact OGO at 1-866-9ASK-OGO or ask-ogo@dhs.gov. All payment related questions should be referred to OJP/OC's Customer Service at 1-800-458-0786 or askoc@ojp.usdoj.gov.

Following acceptance of the grant award and release of any special conditions withholding funds, the Grantee can draw down and expend grant funds through the Automated Standard Application for Payments (ASAP), Phone Activated Paperless Request System (PAPRS) or Letter of Credit Electronic Certification System (LOCES) payment systems. For more information about these options go to <http://www.ojp.usdoj.gov/FinGuide> or call 1-866-9ASK-OGO.

In support of our continuing effort to meet the accelerated financial statement reporting requirements mandated by the U. S. Department of the Treasury and the Office of Management and Budget (OMB), payment processing will be interrupted during the last five (5) **working days** each month. Grantees should make payment requests before the last five working days of the month to avoid delays in deposit of payments.

For example, for the month of June, the last day to request (draw down) payments will be June 23, 2006. Payments requested after June 23, 2006, will be processed when the regular schedule resumes on July 3, 2006. A similar schedule will follow at the end of each month thereafter.

Recipient organizations should request funds based upon immediate disbursement requirements. Funds will not be paid in a lump sum, but rather disbursed over time as project costs are incurred or anticipated. Recipients should time their drawdown requests to ensure that Federal cash on hand is the minimum needed for disbursements to be made immediately or within a few days. Grantees may elect to drawdown funds up to 120 days prior to expenditure/disbursement, in response to the recommendation of the Funding Task Force. DHS strongly encourages recipients to draw down funds as close to expenditure as possible to avoid accruing interest. ***Funds received by grantees must be placed in an interest-bearing account and are subject to the rules outlined in the Uniform Rule 28 CFR Part 66, Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments***, available at:

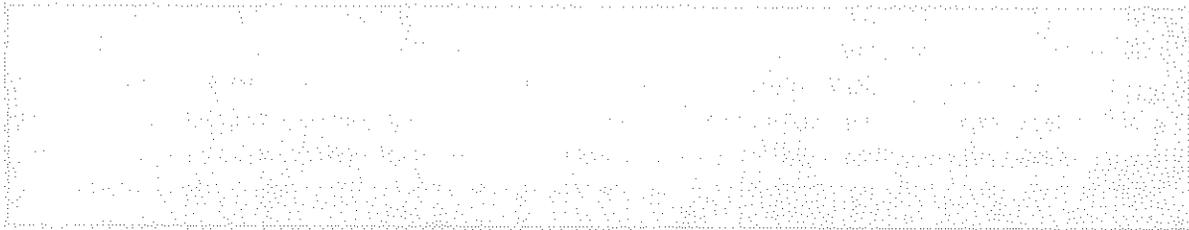
http://www.access.gpo.gov/nara/cfr/waisidx_04/28cfr2_04.html The Uniform Rule 28 CFR Part 70, Uniform Administrative Requirements for Grants and Agreements (Including Subawards) with Institutions of Higher Education, Hospitals and other Non-profit Organizations, at:

http://www.access.gpo.gov/nara/cfr/waisidx_04/28cfr2_04.html. These guidelines

state that entities are required to promptly, but at least quarterly, remit interest earned on advances to:

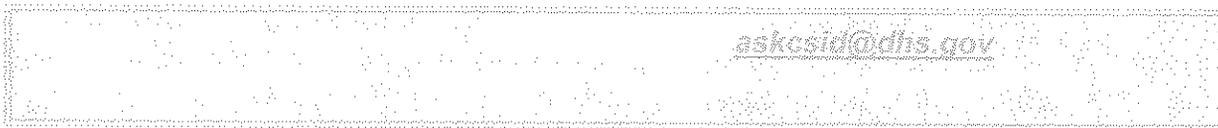
United States Department of Health and Human Services
Division of Payment Management Services
P.O. Box 6021
Rockville, MD 20852

Please consult the OGO *Financial Management Guide* or the applicable OMB Circular for additional guidance.



B. Centralized Scheduling and Information Desk (CSID) Help Line

The CSID is a non-emergency resource for use by emergency responders across the Nation. CSID is a comprehensive coordination, management, information, and scheduling tool developed by DHS through G&T for homeland security terrorism preparedness activities. A non-emergency resource for use by State and local emergency responders across the nation, the CSID provides general information on all G&T programs and information on the characteristics and control of CBRNE, agriculture, cyber materials, defensive equipment, mitigation techniques, and available Federal assets and resources. The CSID maintains a comprehensive database containing key personnel contact information for homeland security terrorism preparedness programs and events. These contacts include personnel at the Federal, State and local levels.



C. Office of Grant Operations (OGO)

G&T's Office of Grant Operations (OGO) will provide fiscal support and fiscal oversight of the grant programs included in this solicitation. All grant and sub grant recipients should refer to the OGO *Financial Management Guide*, available at <http://www.dhs.gov/dhspublic/display?theme=18>.



VI. Reporting, Monitoring and Closeout Requirements

A. Reporting Requirements

The following reports are required of all program participants:

1. Financial Status Reports (FSRs) – Standard Form 269a

Obligations and expenditures must be reported to G&T on a quarterly basis through the FSR, which is due within 30 days of the end of each calendar quarter (e.g., for the quarter ending March 31, FSR is due on April 30).

Please note that this is a change from previous fiscal years. A report must be submitted for every quarter the award is active, including partial calendar quarters, as well as for periods where no grant activity occurs. ***Future awards and fund drawdowns will be withheld if these reports are delinquent.***

FSRs must now be filed online through the Internet at <https://grants.ojp.usdoj.gov>. Forms and instructions can be found at <http://www.ojp.usdoj.gov/oms.htm>.

Grantees are reminded to review the following documents and ensure that grant activities are conducted in accordance with the applicable guidance:

- OMB Circular A-102, Grants and Cooperative Agreements with State and Local Governments, at <http://www.whitehouse.gov/omb/circulars/index.html>;
- OMB Circular A-87, Cost Principles for State, Local, and Indian Tribal Governments, at <http://www.whitehouse.gov/omb/circulars/index.html>;
- OMB Circular A-110, Uniform Administrative Requirements for Grants and Other Agreements with Institutions of Higher Education, Hospitals and Other Non-Profit Organizations, at <http://www.whitehouse.gov/omb/circulars/index.html>;
- OMB Circular A-21, Cost Principles for Educational Institutions, at <http://www.whitehouse.gov/omb/circulars/index.html>; and,
- OMB Circular A-122, Cost Principles for Non-Profit Organizations, at <http://www.whitehouse.gov/omb/circulars/index.html>.

For FY 2006 awards, grant and sub-grant recipients should refer to the OGO Financial Management Guide available at:
<http://www.dhs.gov/dhspublic/display?theme=18>.

All previous awards are still governed by the OJP Financial Guide, available at <http://www.ojp.usdoj.gov/FinGuide>. OGO can be contacted at 1-866-9ASK-OGO or by email at ask-OGO@dhs.gov.

2. Categorical Assistance Progress Report (CAPR)

Following an award, the awardees will be responsible for providing updated obligation and expenditure information on a regular basis. The CAPR is due within 30 days after the end of the reporting period (July 30 for the reporting period of January 1 through June 30, and on January 30 for the reporting period of July 1 through December 31). Future awards and fund drawdowns may be withheld if these reports are delinquent. The final CAPR is due 90 days after the end date of the award period.

Block #12 of the CAPR should be used to note progress against the proposed project. The grantor agency shall provide sufficient information to monitor program implementation and goal achievement. At a minimum, reports should contain the following data: (1) As applicable, the total number of items secured under this grant (e.g., access controls, surveillance, physical enhancements, and vessels) to date, and (2) for other items acquired through this grant, a brief description and total number of items obtained to date.

CAPRs **must be filed online** through the internet at <https://grants.oig.usdoj.gov>. Forms and instructions can be found at <http://www.oig.usdoj.gov/forms.htm>.

3. Financial and Compliance Audit Report

Recipients that expend \$500,000 or more of Federal funds during their fiscal year are required to submit an organization-wide financial and compliance audit report. The audit must be performed in accordance with the Government Accountability Office, *Government Auditing Standards*, located at <http://www.gao.gov/govsujdybk01.nlm>, and *OMB Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations*, located at <http://www.whitehouse.gov/omb/circulars/index.html>. Audit reports are currently due to the Federal Audit Clearinghouse no later than nine months after the end of the recipient's fiscal year. In addition, the Secretary of Homeland Security and the Comptroller General of the United States shall have access to any books, documents, and records of recipients of FY 2006 PSGP assistance for audit and examination purposes provided that, in the opinion of the Secretary of Homeland Security or the Comptroller General, these documents are related to the receipt or use of such assistance. The grantee will also give the sponsoring agency or the Comptroller General, through any authorized representative, access to and the right to examine all records, books, papers or documents related to the grant.

For-profit organizations that expend \$500,000 or more of Federal funds during their fiscal year shall have financial and compliance audits conducted by qualified individuals who are organizationally, personally, and externally independent from those who authorize the expenditure of Federal funds. This audit must be performed in accordance with Government Auditing Standards, 1994 Revision.

The purpose of this audit is to ascertain the effectiveness of the financial management systems and internal procedures that have been established to meet the terms and conditions of the award. Usually, these audits shall be conducted annually, but no less than every two years. The dollar threshold for audit reports established in OMB Circular A-133, as amended, applies.

B. Monitoring

Grant recipients will be monitored periodically by DHS staff, both programmatically and financially, to ensure that the project goals, objectives, timelines, budgets and other related program criteria are being met. Monitoring will be accomplished through a combination of office-based and on-site monitoring visits. Monitoring will involve the review and analysis of the financial, programmatic, and administrative issues relative to each program, and will identify areas where technical assistance and other support may be needed.

The recipient is responsible for monitoring award activities, to include sub awards, to provide reasonable assurance that the Federal award is administered in compliance with requirements. Responsibilities include the accounting of receipts and expenditures, cash management, the maintaining of adequate financial records, and the refunding of expenditures disallowed by audits.

C. Grant Close-out Process

Within 90 days after the end of the grant period, the grantee will submit a final SF-269a and a final CAPR detailing all accomplishments throughout the project. After both of these reports have been reviewed and approved by G&T, a Grant Adjustment Notice (GAN) will be completed to close-out the grant. The GAN will indicate the project as being closed, list any remaining funds that will be de-obligated, and address the requirement of maintaining the grant records for three years from the date of the final SF-269a.



APPENDIX A

AUTHORIZED PROGRAM EXPENDITURES GUIDANCE

Authorized Program Expenditures Guidance

This appendix serves as an additional guide for program expenditure activities. Grantees are encouraged to contact their G&T Program Manager regarding authorized and unauthorized expenditures.

A. Projects that Support the National Port Security Priorities

When developing project proposals for the FY 2006 PSGP, applicants must pay specific attention to the prevention and detection of terrorist attacks which involve IEDs. IEDs pose a threat of great concern to transportation systems across the Nation. IEDs have historically been the terrorist weapon of choice because they combine a high degree of effectiveness with minimal cost. Of greatest concern to port security are IEDs delivered via small craft, underwater and from vehicles on ferries. Particular areas of focus, therefore, should include protection of facilities, including public cruise line and ferry terminals and vessels, from tampering and attack.

The following are examples of security enhancements designed to enhance IED prevention and detection capabilities for port systems:

1. Port Facilities, Including Public Cruise Line and Ferry Terminals

- Explosive Agent Detection Sensors
- Chemical/Biological/Radiological Agent Detection Sensors
- Canines (start-up costs and training for terminal operations)
- Intrusion Detection
- Small boats for State and Local Law Enforcement Marine Patrol/Security Incident Response
- Video Surveillance Systems
- Access Control/Standardized Credentialing
- Improved Lighting
- Secure Gates and Vehicle Barriers
- Floating Protective Barriers
- Underwater Intrusion Detection Systems
- Communications Equipment (including interoperable communications)

2. Vessels and Ferries

- Explosive Agent Detection Sensors
- Chemical/Biological/Radiological Agent Detection Sensors
- Restricted Area Protection (cipher locks, hardened doors, CCTV for bridges and engineering spaces)
- Communications Equipment (including interoperable communications)
- Canines (start-up costs and training for U.S. vehicle/passenger ferries)
- Access Control/Standardized Credentialing
- Floating Protective Barriers

Maritime Domain Awareness (MDA) is the critical enabler that allows leaders at all levels to make effective decisions and act early against a vast array of threats to the security of the United States, its interests, allies, and friends. In support of the National Strategy for Maritime Security, projects that address the enhancement of Knowledge Capabilities (i.e. command, control, communications, and enhanced intelligence sharing and analysis) of the Maritime Domain will be considered for funding.

Areas for Improvements that address MDA include, but are not limited to:

- Surveillance – monitoring of high interest, high value, infrastructure, waterways, and other areas. Sensors may be monitored by live watch standers, keyed to alert based on defined parameters, or monitored by intelligent software.
- Information collection – access to new sources of raw and summary data.
- Decision Support - acquisition of new software tools and services that provide data mining, correlation, threat analysis, anomaly detection, and other decision support products.
- Dissemination – the ability to share data and information including video, radar feeds, intelligence and threat analysis results developed by one entity with all partners within a port.

The following are examples of improvements that address awareness within the Maritime Domain:

- Deployment of access control/standardized credentialing systems (see Section C below for additional guidance)
- Deployment of detection and surveillance equipment
- Development/Enhancement of Information Sharing systems
- Creation/Enhancement of maritime community watch programs
- Construction/Enhancements of Command and Control Facilities
- Enhancement of Interoperable Communications/Asset Tracking

Proposals for MDA systems should be attentive to the following:

- Ensuring that existing surveillance, other sensor, and information systems are appropriately shared and used by all port partners.
- Output of new sensors and data sources should be readily and easily available to all port partners without cost for access. For example, video camera feeds might

be posted to a password protected website that all partners could access. Radar, vessel automated identification systems (AIS) and blue force (port response asset) track outputs should be in an easily translatable format such as xml.

- Systems with an open architecture that can be easily expanded and that can easily interface with other systems should be given preference. Systems that comply with Department of Defense (DoD) Common Operating Environment standards are preferred.
- Addressing needs identified by existing risk assessments. In the coming year the USCG plans to further document and publish its methodology for selecting sensors and sighting. For this year, existing risk assessments and the judgment of the Area Maritime Security Committee (AMSC) and the COTP should be considered when prioritizing needs and developing proposals.

Applicants that are interested in addressing Maritime Domain Awareness are encouraged to familiarize themselves with the National Strategy for Maritime Security: National Plan to Achieve Maritime Domain Awareness. A copy of this document can be found at <http://www.uscg.mil/mda/Docs.htm>.

B. Specific Guidance on Canines

The United States Coast Guard has identified Canine Explosive Detection as the most effective solution for the detection of vehicle borne IEDs. Eligibility for funding of Canine Explosive Detection programs is restricted to U.S. Ferries regulated under 33 CFR Parts 101, 104 & 105 specifically U.S. ferry vessels carrying more than 500 passengers with vehicles, U.S. ferry vessels carrying more than 2,000 passengers and the passenger terminals these specific ferries service. Additionally, only owners and operators of these specific ferries and terminals and port authorities or state, local authorities that provide layered protection for these operations and are defined in the vessel's/terminal's security plans as doing so are eligible.

Eligible Costs: Eligible costs include the purchasing, training and certification of canines; all medical costs associated with initial procurement of canines; kennel cages used for transportation of the canines and other incidentals associated with outfitting and set-up of canines (such as leashes, collars, initial health costs and shots etc.). Eligible costs also include initial training and certification of handlers.

Ineligible Costs: Ineligible costs include but are not limited to hiring, costs associated with handler annual salary, travel and lodging associated with training and certification; meals and incidentals associated with travel for initial certification; vehicles used solely to transport canines; and maintenance / recurring expenses such as annual medical exams, canine food costs, etc.

Certification: Canines used to detect explosives must be certified by an appropriate, qualified organization. Such canines should receive an initial basic training course and also weekly maintenance training sessions thereafter to maintain the certification. The basic training averages 10 weeks for the canine team (handler

and canine together) with weekly training and daily exercising. Comparable training and certification standards, such as those promulgated by the TSA Explosive Detection Canine Program, the National Police Canine Association (NPCA), the United States Police Canine Association (USPCA) or the International Explosive Detection Dog Association (IEDDA) may be used to meet this requirement.⁵

Successful applicants will be required to submit an amendment to their approved Vessel Security Plan as per 33 CFR Part 104.415 detailing the inclusion of a Canine Explosive Detection program into their security measures. Successful applicants will also be required to submit a signed certification to G&T acknowledging that PSGP awards allow a one-time procurement to assist in implementing the Canine Explosive Detection teams. ***The signed certification must be included as a .pdf file attachment to the application in Grants.gov. See Appendix F for the required form.***

Agreement: Applicants are encouraged to thoroughly review the fiscal obligations of maintaining a long-term Canine Explosive Detection program. If applicable, successful applicants will be required to submit an amendment to their approved Vessel Security Plan as per 33 CFR Code of Federal Regulation, Part 104.415 detailing the inclusion of a Canine Explosive Detection program into their security measures. Successful applicants will be required to submit a signed certification to G&T acknowledging that PSGP awards allow a one-time procurement to assist in implementing the Canine Explosive Detection teams. This one-time procurement authorization will be issued with the understanding that the applicant will maintain the canine's proficiency for explosives detection, and that any additional costs throughout the 8 to 10 year service life of the canine are the sole responsibility of the applicant.

Additional Resources Available for Canine Costs: DHS is aware that the financial obligations of a Canine Explosive Detection Program can be burdensome. ***The Port Security Grant Program, while providing the ability to defray the majority of start up costs, does not cover any recurring costs associated with such programs. However, the Transit Security Grant Program (TSGP) and Homeland Security Grant Program (HSGP) are two additional DHS grant programs that can provide funding for certain operational costs associated with heightened states of alert within the port area and nationally.*** DHS strongly encourages applicants to investigate their eligibility for these resources when developing their canine programs.

<http://www.grants.gov>

⁵ Training and certification information can be found at: <http://www.tsa.gov/publicdisplay/11home03>, <http://www.uspcanine.org>, <http://www.uspcanine.com/indprod/washdc>, and <http://www.bonobdog.org>.

C. Specific Guidance on Employee Identification

The Transportation Worker Identification Credential (TWIC) is designed to be an open architecture, standards-based system and follow published ANSI/NIST and ISO standards. Accordingly, port projects that involve new installations/upgrades to access control/credentialing systems, should exhibit compliance to these and related standards in their system design and implementation. Port card reader systems should be compliant with ISO 7816 and/or ISO 14443 for basic TWIC smart card compatibility. The TWIC program will enable the use of biometric recognition technologies in port access control systems, following guidelines provided by the ANSI INCITS 383-2004 "Biometric Profile -Interoperability and Data Interchange -Biometrics based Verification and Identification of Transportation Workers" document. The TWIC program will be compliant to the GSC-IS (Government Smart Card Interoperability Standard), and associated efforts that include the GSC-IAB (Government Smart Card-Interagency Advisory Board) PAIIWG (Physical Access Interagency Interoperability Working Group) technical implementation guidelines and data models.

D. Specific Guidance on Lighting

All lighting must meet Occupational Safety and Health Administration (OSHA) requirements.

E. Specific Guidance on Sonar Devices

DHS has determined certain sonar devices that will not damage the environment or require special permitting under the National Environmental Policy Act are eligible for funding under the PSGP. The four types of allowable sonar devices are: imaging sonar, scanning sonar, side scan sonar, and 3-dimensional sonar. These types of sonar devices are intended to support the detection of underwater improvised explosive devices (IED) and enhance Maritime Domain Awareness. The eligible types of sonar, and short descriptions of their capabilities, are provided below:

Imaging Sonar: A high-frequency sonar that produces "video-like" imagery using a narrow field of view. The sonar system can be pole-mounted over the side of a craft or hand carried by a diver.

Scanning Sonar: Consists of smaller sonar systems that can be mounted on tripods and lowered to the bottom of the waterway. Scanning sonar produces a panoramic view of the surrounding area and can cover up to 360 degrees.

Side Scan Sonar: Placed inside of a shell and towed behind a vessel. Side scan sonar produces strip-like images from both sides of the device.

3-Dimensional Sonar: Produces 3-dimensional imagery of objects using an array receiver.

F. Specific Guidance on Security Operational and Maintenance Costs

In accordance with 46 USC Sec. 70107(b)(2), the cost of acquisition, operation, and maintenance of security equipment or facilities to be used for security monitoring and recording, security gates and fencing, marine barriers for designated security zones, security-related lighting systems remote surveillance, concealed video systems, security vessels, and other security-related infrastructure or equipment that contributes to the overall security of passengers, cargo, or crewmembers are allowable. In addition, routine maintenance costs for security monitoring, such as the cost of tapes for recording, are allowable. *However, as indicated in Section IV: Program and Application Requirements, business operations and maintenance costs, such as personnel costs and items generally characterized as indirect or "overhead" costs, are unallowable.*

G. Specific Guidance on Vulnerability Assessment Costs

In accordance with 46 USC Sec. 70107(b)(4), the cost of conducting vulnerability assessments to evaluate and make recommendations with respect to security is an eligible cost under the FY 2006 PSGP. *However, as indicated in Section IV: Program and Application Requirements, the development of new risk/vulnerability assessment models and methodologies is unallowable.*

H. Specific Guidance on Training and Exercises

Training: Port Security Training will be limited to only those courses that have been approved by the Maritime Administration (MARAD) and the U.S. Coast Guard, or the DHS Office of Grants and Training. More information can be obtained at: <http://marad.dot.gov/MTSA/MARAD%20Web%20Site%20for%20MTSA%20Course.html> and <http://www.uscg.mil/stow/security.pdf>

Exercises: Funding used for Port Security Exercises will only be permitted for those exercises that are in direct support of a facility or port area's MTSA required exercises. These exercises must be coordinated with the COTP and AMSC and adhere to the guidelines outlined in DHS Homeland Security Exercise and Evaluation Program (HSEEP).

I. Specific Guidance on Management and Administrative (M&A) Costs

PSGP funds may be used for the following M&A costs:

- **Hiring of full-time or part-time staff or contractors/consultants:**
 - To assist with the management of the FY 2006 PSGP;
- **Travel expenses:**
 - To assist with the management of the FY 2006 PSGP;
- **Meeting-related expenses:**
 - To assist with the management of the FY 2006 PSGP.

<http://www.dhs.gov/dhspublic/display?theme=18&content=4206>

APPENDIX B

PORT SYSTEM OVERVIEW TEMPLATE GUIDANCE

Port System Overview Template Guidance

The Port System Overview must not exceed 10 pages. Applicants should follow the format below for this file attachment.

Area of Operations:

- Identify COTP Zone
- Identify eligible port, as listed in Table 1

Point(s) of Contact for Organization:

- Identify the organization's Authorizing Official for entering into grant agreement.
- Identify the organization's primary point of contact for management of the project(s).

Ownership/Operation:

- Identify whether the applicant is: (1) a private entity, (2) a state or local agency; or (3) a consortium composed of local stakeholder groups (i.e., river groups, ports, and terminal associations) representing federally regulated ports, terminals, U.S. inspected passenger vessels, or ferries.

Role in Providing Layered Protection of Regulated Entities (applicable to state or local agencies, consortia, and associations only):

- Identify the specific regulated entities to which you are providing layered protection.
- Describe your organization's specific roles, responsibilities, and activities in delivering layered protection.

Infrastructure:

- Describe the type, quantity, and significance of infrastructure to be protected through the prospective grant. Identify who it is owned or operated by, if not by your own organization.

IED Capabilities:

Clearly describe your organization's current prevention and detection capabilities relative to IEDs. IED capabilities and activities include:

- Intelligence and deterrence operations
- Inspection capabilities, including:
 - Explosive Agent Detection Sensors
 - Chemical/Biological/Radiological Agent Detection Sensors
 - Canines
- Improved surveillance and security operations, including:
 - Video Surveillance Systems
 - Small boats for State and Local Law Enforcement Marine Patrol/Security Incident Response
- Investigations