U.S. DEPARTMENT OF HOMELAND SECURITY

Fiscal Year 2007
INFRASTRUCTURE PROTECTION PROGRAM:

PORT SECURITY GRANT PROGRAM

PROGRAM GUIDANCE AND APPLICATION KIT

January 2007

OFFICE OF GRANTS AND TRAINING

KEY CHANGES IN FY 2007

The Fiscal Year 2007 (FY07) Infrastructure Protection Program (IPP) contains significant improvements based upon extensive outreach to FY06 IPP participants and stakeholders. In addition, the risk analysis assessments that form the basis for eligibility under the IPP have been simplified, refined and considerably strengthened.

The pool of eligible port applicants has been expanded to reflect the changes required by the SAFE Port Act, which states all entities covered by an Area Maritime Security Plan (AMSP) may submit an application for consideration. In addition, in a number of cases, port areas have been grouped together to reflect geographic proximity, shared risk and a common waterway.

Potential applicants will have more time this year to complete the application process. The Department of Homeland Security (DHS) has also created multiple opportunities for applicants to have consultations with the Department's grant program and subject matter experts prior to the point of application final review. Some of the IPP grants will be executed as cooperative agreements, thus allowing for iterative refinements regarding an applicant's funding proposal in order to maximize effective communication between DHS and our external partners about these important homeland security investments.

This year's IPP grants strengthen DHS's ability to protect security- and business-sensitive information that will be provided with grant applications from inappropriate public release. To increase program flexibility, the period for compliance under IPP grants has been extended from 30 to 36 months. New federal legislation requires compliance with federal energy policy laws and certain other administrative requirements.

As with the other DHS's infrastructure grant programs, the largest portion of the port grant dollars will again be awarded to the highest risk facilities and for projects that offer the maximum return on investment for risk reduction.

All applicants are required to read and conform to all requirements of the grant guidance documents and must have read and accepted the Program Guidance as binding.

CONTENTS

INTRODUCTION

The Port Security Grant Program (PSGP) is one of six grant programs that constitute the Department of Homeland Security Fiscal Year 2007 Infrastructure Protection Program (IPP).[1] The IPP is one tool among a comprehensive set of measures authorized by Congress and implemented by the Administration to help strengthen the nation's critical infrastructure against risks associated with potential terrorist attacks.

The vast bulk of America's critical infrastructure is owned and/or operated by state, local and private sector partners. The funds provided by the PSGP are primarily intended to support the work of increasing port-wide risk management, enhanced domain awareness, capabilities to prevent, detect, respond to and recover from attacks involving improvised explosive devices (IEDs) and other non-conventional weapons, as well as training and exercises.

The purpose of this package is to provide: (1) an overview of the PSGP; and (2) the formal grant guidance and application materials needed to apply for funding under the program. Also included is an explanation of DHS management requirements for implementation of a successful application.

Making an application for significant Federal funds under programs such as this can be quite complex and occasionally frustrating. Our job at DHS is to provide clear guidance and efficient application tools to assist applicants. Our customers are entitled to effective assistance during the application process, and transparent, disciplined management controls to support grant awards. We intend to be good stewards of precious Federal resources, and commonsense partners with our state and local colleagues.

We understand that individual port areas will have unique needs and tested experience about how best to reduce risk locally. Our subject matter experts will come to the task with a sense of urgency to reduce risk, but also with an ability to listen carefully to local needs and approaches. In short, we commit to respect flexibility and local innovation as we fund national homeland security priorities.

A. Federal Investment Strategy.

The IPP is an important part of the Administration's larger, coordinated effort to strengthen homeland security preparedness, including the security of America's critical infrastructure. The IPP implements objectives addressed in a series of post 9/11 laws, strategy documents, plans, Executive Orders and Homeland Security Presidential Directives (HSPDs) outlined in Appendix 1. Of particular significance are the National Preparedness Goal and its associated work products, including the National

[1] The IPP's other components include grants targeted for transit systems (including intercity passenger rail and ferry systems), intercity bus companies, the trucking industry's Highway Watch® program and the Buffer Zone Protection Program for other high-risk infrastructure facilities.

Infrastructure Protection Plan and its forthcoming sector-specific plans. The National Preparedness Goal is an all-hazards vision regarding the nation's four core preparedness objectives: prevent, protect, respond and recover from both terrorist attacks and catastrophic natural disasters.

The National Preparedness Goal defines a vision of what to accomplish and a set of tools – including IPP grant investments – to forge a unified national consensus about what to do and how to work together at the Federal, State, local, and tribal levels. Private sector participation is integral to the Goal's success.[2] It outlines 15 scenarios of terrorist attacks or national disasters that form the basis of much of the Federal exercise and training regime. In addition, it identifies some 37 critical capabilities that DHS is making the focus of key investments with State, local and tribal partners.

DHS expects its critical infrastructure partners – including recipients of IPP grants – to be familiar with this national preparedness architecture and to incorporate elements of this architecture into their planning, operations and investment to the degree practicable. Our funding priorities outlined in this document reflect National Preparedness Goal priority investments as appropriate. Programmatic requirements or priority investment categories reflecting the national preparedness architecture for this IPP grant program are expressly identified below.

B. Funding Priorities.

The funding priorities for the FY07 PSGP reflect the Department's overall investment strategy, in which two priorities have been paramount: risk-based funding and regional security cooperation.

First, and based upon ongoing intelligence analysis, extensive security reviews, consultations with port industry partners and Congressional direction, DHS will again focus the bulk of its available port grant dollars on the highest-risk port systems. Eligible port areas were identified using a comprehensive, empirically-grounded risk analysis model that is described below in the section regarding eligible recipients.

At the recommendation of the United States Coast Guard (USCG), in several cases multiple port areas have been grouped together to reflect geographic proximity, shared risk and a common waterway. As with other DHS grant programs, applications from these port clusters must be coordinated locally to reflect integrated security proposals to use PSGP grant dollars. Eight port regions, identified below, have been selected as Tier I (highest risk) ports. Each Tier I port area has been designated a specific amount of money for which eligible entities within that port area may apply.

[2] The National Preparedness Goal and its supporting documents were published in draft form in March 2005. After extensive stakeholder outreach, the final Goal documents are expected to be published early in 2007. For purposes of aligning applications under the IPP, applicants can rely on the existing draft Goal, available at: *http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm* .

In addition, all port areas not identified in Tier I are eligible for FY07 PSGP as Tier II, III, or IV applicants. The Tier II, III, and IV ports will compete for funding drawn from their respective pool of applicants.

DHS plans an extensive amount of outreach and support to applicant agencies to answer any questions about PSGP program requirements, and to assist port areas with filing the strongest possible applications. Locally, Coast Guard's Captain of the Port (COTP) will take the lead in coordinating this process and will also participate in review of applications.

Second, DHS places a very high priority on ensuring that all PSGP applications reflect robust regional coordination and an investment strategy that institutionalizes regional security strategy integration. This priority is a core component in the Department's statewide grant programs and the Urban Area Security Initiative grants.

During FY07, DHS will continue its effort to encourage and help coordinate port security planning efforts, such as the Area Maritime Security Plans (AMSPs),with complementary initiatives underway at the State and Urban Area levels. This will also be the focus of an important evolution in the focus of the PSGP -- from a program that is primarily focused on the security of individual facilities within ports, to a port-wide risk management program that is fully integrated into the broader regional planning construct that forms the core of the Urban Area Security Initiative (UASI), as well as applicable statewide initiatives. Adoption of a deliberate risk management planning process, consistent with that employed in the UASI and state programs, is also a key focus of the recently signed SAFE Port Act. This emphasis is embedded in our FY07 PSGP, and DHS efforts will increase in this area during this year.

In addition to these two overarching priorities, the Department identifies the following five specific priorities as our highest priority selection criteria for the FY07 PSGP:

1. **Enhancing Maritime Domain Awareness (MDA).** MDA is the critical enabler that allows leaders at all levels to make effective decisions and act early against threats to the security of the Nation's seaports. In support of the National Strategy for Maritime Security, port areas should seek to enhance their MDA through projects that address knowledge capabilities within the maritime domain (e.g., access control/standardized credentialing, command and control, communications and enhanced intelligence sharing and analysis).

2. **Enhancing prevention, protection, response and recovery capabilities.** Port areas should seek to enhance their capabilities to prevent, detect, respond to and recover from terrorist attacks employing improvised explosive devices (IEDs), as well as attacks that employ other non-conventional weapons. Of particular concern in the port environment are attacks that employ IEDs delivered via small craft (similar to the attack on the USS Cole), by underwater swimmers (such as underwater mines) or on ferries (both passenger and vehicle).

3. **Training and exercises.** Port areas should seek to ensure that appropriate capabilities exist among staff and managers, and regularly test these capabilities through a program of emergency drills and exercises. Emergency drills and exercises (such as the TSA Port Security Exercise Training Program) test operational protocols that would be implemented in the event of a terrorist attack, and consist of live situational exercises involving various threat and disaster scenarios, table top exercises, and methods for implementing lessons learned.

4. **Efforts supporting implementation of the Transportation Worker Identification Credential (TWIC).** The TWIC is a Congressionally-mandated security program by which DHS will conduct appropriate background investigations and issue biometrically enabled and secure identification cards for individuals requiring unescorted access to U.S. port facilities. Regulations outlining the initial phase of this program (card issuance) were issued by the Transportation Security Administration (TSA) in cooperation with the Coast Guard on January 1, 2007. Additional detail about the TWIC program is found in Appendix 2.

5. **Efforts in support of the national preparedness architecture**. Port areas are encouraged to take steps to embrace any of the national preparedness architecture priorities, several of which have already been highlighted as priorities. The following six national priorities are particularly relevant: expanding regional collaboration; implementing as appropriate elements of the National Strategy for Maritime Security, the National Incident Management System, the National Response Plan and the National Infrastructure Protection Plan and its corresponding Transportation Sector Security Plan; strengthening information sharing and collaboration capabilities; enhancing interoperable communications capabilities; strengthening CBRNE detection and response capabilities; and improving planning and citizen preparedness capabilities.[3]

D. Allowable Expenses.

Specific investments made in support of the funding priorities discussed above generally fall into one of four categories. FY07 PSGP allowable costs are therefore divided into the following four categories:

1. Maritime Domain Awareness
2. IED prevention, protection, response and recovery capabilities
3. Training and exercises
4. Management and administration

Appendix 2 provides additional detail about each of these four allowable expense categories, additional guidance on other allowable costs (i.e. guidance on canines, employee identification programs, etc.), as well as a section that identifies several specifically unallowed cost items.

[3] For more information, see the Citizen Corps website at *http://www.citizencorps.gov/*.

PART I.
AVAILABLE FUNDING AND ELIGIBLE APPLICANTS

This section summarizes the total amount of funding available under the FY07 PSGP, the basic distribution method used to administer the grants and the port areas that are eligible for FY07 funding.

A. Available Funding.

In FY07, the total amount of funds distributed under the PSGP will be $201.17 million. This is up from $168.05 million distributed in FY06. The available funding will be divided into four pools, as summarized in Table 1.

Table 1.
PSGP FY07 Available Funding ($ millions)

Tier	FY07 Funding
Tier I	$120,702,000
Tier II	$40,234,000
Tier III	$30,175,500
Tier IV	$10,058,500
TOTAL	**$201,170,000**

Applicants are encouraged <u>not</u> to request more than two times the average percentage of IPP funds received annually from FY03 through FY06.[4] While this requested "cap" is not a mandatory application limitation, by exercising this restraint applicants will speed the grant review cycle, make their core investment priorities and capabilities more clear, and increase the likelihood of receiving full project funding for realistic applications. Historically, the PSGP has provided full funding for proposed PSPG projects at a given port, rather than partial project funding. Each year, at least several ports have received no funding for projects because they made such expensive requests that funding was unavailable to cover the total project cost.

B. Selection of Eligible Applicants.

The FY07 DHS Appropriations Act provides funds for a competitive grant program to address physical security enhancements for critical national seaports. Port areas for the FY07 PSGP were identified using comprehensive, empirically-grounded risk analysis modeling. The risk methodology for the IPP programs is consistent across the

[4] Applicants that have not previously received PSGP funding should prudently calibrate potential application amounts against funds available for the relevant eligibility tier.

modes and is linked to the risk methodology used to determine eligibility for the core DHS State and local grant programs.

Within the PSGP, eligibility for all grant awards is first predicated on a systematic risk analysis that compares all of the eligible port areas and rates eligible ports in a given area for comparative risk. Then all port areas will be comparably rated. The FY07 risk assessment formula was further strengthened and refined from last year's risk assessment formula.

The PSGP risk formula is based on a 100 point scale comprised of ***threat*** (20 points) and ***vulnerability/consequences*** (80 points). Risk data for eligible port areas is gathered individually and then aggregated by region. The DHS risk formula incorporates multiple normalized variables, meaning that for a given variable, all eligible port areas are empirically ranked on a relative scale from lowest to highest.

The DHS risk assessment methodology for PSPG considers critical infrastructure system assets, and characteristics that might contribute to their risk in four groupings: (1) intelligence community assessments of threat; (2) economic consequences of attack; (3) port assets; and (4) area risk (to people and physical infrastructure immediately surrounding the port). The relative weighting of variables reflects DHS's overall risk assessment, and the FY07 program priorities described above. Specific variables include multiple data sets regarding: international cargo value and measures of cargo throughput (container, breakbulk, international and domestic); length of port channel; military mission variables; adjacent critical asset inventories; and Coast Guard Maritime Security Risk Analysis Model (MSRAM) data.

C. Eligible Applicants.

The recently passed SAFE Port Act states that all entities covered by an AMSP[5] may submit an application for consideration of funding. However, Congress has also specifically directed DHS to apply these funds to the highest risk ports. In support of this, the PSGP includes a total of 102 specifically identified critical ports, representing approximately 95 percent of the foreign waterborne commerce of the United States. Based upon Coast Guard recommendations, these ports are aggregated into 72 discreet port funding areas. As described below, all other ports covered by an AMSP (Tier IV ports) are eligible to apply for grants from a PSGP funding pool created for that purpose. In addition, another IPP grant program will fund security measures for certain identified ferry systems.

Within the PSGP, the following entities are specifically encouraged to apply:

- Owners or operators of federally regulated terminals, facilities, U.S. inspected passenger vessels or ferries as defined in the Maritime Transportation Security Act (MTSA) 33 Code of Federal Regulations (CFR) Parts 101, 104, 105, and 106.

[5] For purposes of the FY07 PSGP, a facility that is not expressly identified in an AMSP will be considered covered under an AMSP if the facility in question has had a risk analysis completed by the US Coast Guard utilizing the MSRAM tool.

- Port authorities or other State and local agencies that provide layered security[6] protection to federally regulated facilities in accordance with an AMSP or a facility or vessel security plan

- 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

Table 2 summarizes the specific port areas that are eligible for funding through the FY07 PSGP by tier. Tier I regions are provided with an amount of risk-based funding from the $120.7 million available to them (listed below) that they are eligible to apply for and approved grants will be executed by cooperative agreement. Tier II through Tier IV port areas may compete for the remainder of eligible funding identified in the corresponding tier -- $80.5 million. ***Presence on this list does not guarantee grant funding.***

Table 2.
Eligible Port Areas Systems

Tier	State	Port Area	FY07 Allocation
I	CA	**Bay Area** Oakland Richmond San Francisco Stockton	$11,201,793
		Los Angeles-Long Beach Long Beach Los Angeles	$14,723,942
	DE/NJ/PA	**Delaware Bay** Camden Chester Marcus Hook Paulsboro Penn Manor Philadelphia Wilmington	$11,331,328
	LA	**New Orleans** Baton Rouge New Orleans Plaquemines South Louisiana	$17,330,180
	NY/NJ	**New York/New Jersey**	$27,178,581

[6] For purposes of the FY07 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. There are three kinds of organizations that provide port-wide layered security: a port authority, state and local governments, and consortia or associations that represent MTSA regulated entities as defined in 33 CFR Parts 101, 104, 105 and 106.

Tier	State	Port Area	FY07 Allocation
	TX	**Houston-Galveston** Galveston Houston Texas City	$15,720,981
		Sabine-Neches River Beaumont Port Arthur	$10,961,035
	WA	**Puget Sound** Anacortes Everett Seattle Tacoma	$12,254,160
II	AL	**Mobile**	$40,234,000
	FL	**Jacksonville**	
	GA	**Savannah**	
	IL/IN	**Southern Tip of Lake Michigan** Burns Harbor Chicago Gary Indiana Harbor	
	KY	**Louisville**	
	LA	**Lake Charles**	
	MD	**Baltimore**	
	MA	**Boston**	
	MO	**St. Louis**	
	OH	**Cincinnati**	
	OR/WA	**Columbia-Willamette River System** Kalama Longview Portland Vancouver	
	PA	**Pittsburgh**	
	SC	**Charleston**	
	TN	**Memphis**	
	TX	**Corpus Christi**	
	VA	**Hampton Roads**	
		Newport News	
		Norfolk Harbor	
	WV	**Huntington**	
III	AL	**Guntersville**	$30,175,500
	AK	**Anchorage**	
		Valdez	
	AR	**Helena**	
	CA	**Port Hueneme**	
		San Diego	
	CT	**Long Island Sound** Bridgeport New Haven New London	
	FL	**Miami**	
		Palm Beach	
		Panama City	
		Pensacola	
		Port Canaveral	
		Port Everglades	
		Tampa Bay	
		Port Manatee	
		Tampa	

Tier	State	Port Area	FY07 Allocation
	GU	**Apra Harbor**	
	HI	**Honolulu**	
	IN	**Mount Vernon**	
	LA	**Port Fourchon/LOOP**	
	ME	**Portland**	
	MI	**Detroit**	
	MN	**Minneapolis-St. Paul** Minneapolis St. Paul	
		Two Harbors	
	MN/WI	**Duluth-Superior**	
	MS	**Greenville**	
		Gulfport	
		Pascagoula	
		Vicksburg	
	MO	**Kansas City**	
	NH	**Portsmouth**	
	NY	**Albany**	
		Buffalo	
	NC	**Morehead City**	
		Wilmington	
	OH	**Cleveland**	
		Toledo	
	OK	**Tulsa**	
	PR	**Ponce**	
		San Juan	
	RI	**Providence**	
	TN	**Chattanooga**	
		Nashville	
	TX	**Brownsville**	
		Freeport	
		Matagorda	
		Victoria	
	WI	**Green Bay**	
		Milwaukee	
IV	**Eligible entities not located within one of the port areas identified above, but operating under an Area Maritime Security Plan, are eligible to compete for funding within Tier IV.**		$10,058,500
		Total FY07 PSGP Allocation	$201,170,000

PART II.
APPLICATION EVALUATION PROCESS

This section summarizes the roles and responsibilities within DHS for managing the PSGP, the overall timetable for the FY07 program, and core process and priorities that will be used to assess applications under the FY07 PSGP. The next section provides detailed information about specific application requirements and the process for submission of applications.

A. PSGP Program Management: Roles and Responsibilities at DHS.

Within DHS, the Coast Guard by law has the lead for managing the Department's security oversight and security programs for the port industry. USCG provides port subject matter expertise within DHS and determines the primary security architecture for the PSGP program. Its subject matter experts have the lead in crafting all selection criteria associated with the application review process. Regarding some matters, such as the TWIC program, the USCG and the Transportation Security Administration and/or the U.S. Customs and Border Protection (CBP) will work together for program management. The USCG's Intel Coordination Center will coordinate daily with DHS Chief Intelligence Officer to review and craft intelligence assessments for the maritime portion of the transportation sector.[7]

The Department's Grants and Training (G&T) organization has the lead for designing and operating the administrative mechanisms needed to manage the Department's core grant programs, including this IPP grant program. In short, G&T is responsible for ensuring compliance with all relevant Federal grant management requirements and delivering the appropriate grant management tools, financial controls, audits and program management discipline needed to support the PSGP. While both USCG and G&T of necessity interface directly with our port stakeholders, the Coast Guard will have the lead on matters related to prioritizing specific investments and setting security priorities associated with PSGP.

Effective management of the PSGP entails a partnership within DHS, the boundaries of which have been defined by DHS Secretary Chertoff. In order to make this partnership seamless to our external partners, upon award of a FY07 PSGP grant, each grantee will be provided two individuals who will serve as primary account managers -- one individual from USCG and one from G&T. These two individuals will be assigned to be turnkey facilitators for our grant recipients. They will meet directly with grantees as needed, and will coordinate with each other routinely to facilitate support for the grantees in a given region. These individuals will be the one-stop PSGP account managers for our port industry customers.

[7] TSA and CBP also coordinate regularly with USCG and with other DHS components regarding intelligence assessments relevant to maritime security.

B. Overview -- Application Deadline and Review Process.

Completed Applications must be submitted to DHS via *grants.gov* (see below for details about this Federal grants application tool) *no later than 11:59 PM EST, March 6, 2007.*

Applicants must comply with all administrative requirements -- including Investment Justifications, budgets and application process requirements -- described herein. Having met all administrative requirements, Tier II-IV applications will be subject to a series of reviews by local and national subject matter experts to ensure the most effective distribution of funding among the eligible applicants and appropriate coordination with regional and state homeland security planning efforts.

1. **Initial Screening.** USCG and G&T will conduct an initial review of all FY07 PSGP applications. Applications passing this review will be grouped by port area and provided to the applicable COTP for further review. *Note: Applicants will be given a time-limited opportunity to address clerical errors (such as missing file attachments, misnamed files, etc.) identified during the initial screening process.*

2. **Field Review.** Field level reviews will be managed by the applicable COTP in coordination with the U.S. Department of Transportation Maritime Administration's 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 also coordinate the results of the field review with the applicable State Administrative Agency or Agencies and State Homeland Security Advisor(s). For each port, the COTP will submit to DHS evaluations that include the following: (1) each specific application is scored for compliance with the four core grant program criteria enumerated below, and a total score is computed; and (2) all proposals received from each port is ranked from highest to lowest in terms of their contributions to risk reduction and cost effectiveness.

   2.1 The four core PSGP criteria are as follows:

   - **Criteria #1**. Projects that support PSGP Funding Priorities identified in this *Program Guidance and Application Kit* package:
     - Enhancement of the port area's MDA (e.g., access control/standardized credentialing, command and control, communications and enhanced intelligence sharing and analysis).
     - Enhancement of the port area's prevention, protection, response and recovery capabilities (e.g., capabilities that would help mitigate potential IED attacks via small craft and underwater swimmers or onboard passenger and vehicle ferries).

  - Training and exercises (e.g., training programs to ensure an appropriate level of capability on the part of port staff and management, exercises that test the ability of the port area to prevent, detect, respond to and recover from potential terrorist attacks).

  - TWIC implementation projects.

  - Efforts in support of the national preparedness architecture.

- **Criteria #2***.* Projects that address priorities outlined in the applicable AMSP, as mandated under the MTSA.

- **Criteria #3***.* Projects that address additional security priorities based on the COTP's expertise and experience with the specific port area.

- **Criteria #4***.* Projects that offer the highest potential for risk reduction for the least cost.

After completing field reviews, COTPs will submit the field review project scores and prioritized lists to G&T to begin coordination of the national review process for Tier II-IV applicants. Tier I applicants will be finalized using a cooperative agreement.

3. **National Review.** Following the field review, a National Review Panel will be convened with subject matter experts drawn from the USCG, TSA, G&T, CBP, the DHS Office of Infrastructure Protection, the DHS Domestic Nuclear Detection Office and the U.S. Department of Transportation's MARAD. The purpose of the National Review 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.[8]

   A risk-based algorithm will then be applied to the National Review Panel's validated, prioritized list for each Tier II-IV port area. The algorithm 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.

[8] The National Review Panel will have the ability to recommend partial funding for individual projects and eliminate others that are determined to be duplicative or require a sustained Federal commitment to fully realize the intended risk mitigation. The National Review Panel will also validate proposed project costs. Decisions to reduce requested funding amounts or eliminate requested items deemed inappropriate under the scope of the FY07 PSGP will take into consideration the ability of the revised project to address the intended national port security priorities and achieve the intended risk mitigation goal. Historically, the PSGP has placed a high priority on providing full project funding rather than partial funding.

- Relationship of the project to the local port security priorities.
- COTP ranking (based on each COTP's prioritized list of projects).
- Risk level of the port area in which the project would be located (based on a comprehensive risk analysis performed by DHS).

The National Review Panel will be asked to evaluate and validate the consolidated and ranked project list resulting from application of the algorithm. Awards will be made based on the final ranked list of projects identified by the National Review Panel.

C. Grant Application Support from DHS.

During the application period, and in conjunction with industry associations, DHS will identify multiple opportunities for a cooperative dialogue between the Department and potential applicants. This commitment is intended to ensure a common understanding of the funding priorities and administrative requirements associated with the FY07 PSGP, and to help in submission of projects that will have the highest impact on reducing risks for the transit systems and their customers.

PART III.
PROGRAM REQUIREMENTS

This section provides detailed information about specific application requirements and the process for submission of applications.

A. General Program Requirements.

Successful FY07 PSGP applicants must comply with the following general requirements:

1. **Management and Administration limits.** A maximum of 3 percent may be retained by the applicant, and any funds retained are to be used solely for management and administrative purposes associated with the PSGP award.

2. **Match requirement.** The following match requirements apply for the FY07 PSGP:

   - **Public Sector*.*** Public sector applicants must provide matching funds supporting at least ***25 percent of the total project cost*** for each proposed project.[9]

   - **Private Sector*.*** 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).

B. Application Requirements.

The following steps must be completed using the on-line *grants.gov* system to ensure a successful application submission:

1. **Application via *grants.gov*.** DHS participates in the Administration's e-government initiative. As part of that initiative, all IPP applicants must file their applications using the Administration's common electronic "storefront" -- *grants.gov*. Eligible applicants must apply for funding through this portal, accessible on the Internet at *http://www.grants.gov*.

[9] Applications for consortia projects submitted by public entities (where the consortia include both public and private entities) must demonstrate a 25 percent cash match.

2. **Application deadline**. Completed Applications must be submitted to Grants.gov no later than **11:59 PM EST, March 6, 2007**.

3. **Valid Central Contractor Registry (CCR) Registration**. The application process also involves an updated and current registration by the applicant and the applicant's Business Point of Contact through the Central Contractor Registry (CCR). Eligible applicants must confirm CCR registration at *http://www.ccr.gov*, as well as apply for FY07 IPP funding through *grants.gov* at *http://www.grants.gov*.

   While registration with Grants.gov and the CCR is a one-time process, new applicants are strongly encouraged to complete their registrations at least ten days prior to the March 6, 2007 application deadline.

4. **On-line application.** The on-line application must be completed and submitted using Grants.gov after CCR registration is confirmed. The on-line application includes the following required forms and submissions:

   - Standard Form 424, Application for Federal Assistance
   - Standard Form 424B Assurances
   - Standard Form LLL, Disclosure of Lobbying Activities
   - Standard Form 424A, Budget Information
   - Certification Regarding Debarment, Suspension, and Other Responsibility Matters
   - Any additional Required Attachments

   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.

5. **Project period.** The project period will be for a period not to exceed 36 months.

6. **DUNS number**. The applicant must provide a Dun and Bradstreet Data Universal Numbering System (DUNS) number with their application. This number is a required field within *grants.gov* and for CCR Registration. Organizations should verify that they have a DUNS number, or take the steps necessary to obtain one, as soon as possible. Applicants can receive a DUNS number at no cost by calling the dedicated toll-free DUNS Number request line at 1-800-333-0505.

7. **Investment Justifications.** As part of the application process, applicants must develop a formal Investment Justification that addresses each initiative proposed for funding. These Investment Justifications must demonstrate how proposed projects address gaps and deficiencies in current programs and capabilities. Additional details and templates or the Investment Justification may be found in Appendix 4.

   Applicants may propose up to up to three investments within their Investment Justification. The individual investments 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 investments in each port area.

8. **Detailed budget**. The applicant must also provide a detailed budget for the funds requested. 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 and any appropriate narrative. The budget should also demonstrate any match. Additional details and templates for the Detailed Budget may be found in Appendix 5.

9. **Memorandum of Understanding/Memorandum of Agreement (MOU/MOA) Requirement**. State and local agencies, as well as consortia or associations that 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. This information may be provided using one of the attachment fields within *grants.gov*. Additional details and a suggested MOU/MOA template may be found in Appendix 6.

10. **Standard financial requirements.**

    10.1 -- Non-supplanting certification. This certification affirms that grant funds will be used to supplement existing funds, and will not replace (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.

    10.2 – 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.

    10.3 -- 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.*

10.4 -- Accounting System and Financial Capability Questionnaire. All nongovernmental (non-profit and commercial) organizations that apply for IPP funding that have not previously (or within the last 3 years) received funding from G&T must complete the Accounting System and Financial Capability Questionnaire. The form can be found at *http://www.ojp.usdoj.gov/oc*.

11. Technology requirements.

11.1 -- National Information Exchange Model. To support homeland security, public safety, and justice information sharing, G&T requires all grantees to use the latest National Information Exchange Model (NIEM) specifications and guidelines regarding the use of XML for all IPP awards. Further information about the required use of NIEM specifications and guidelines is available at *http://www.niem.gov*.

11.2 -- 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). State, local, and industry partners are increasingly incorporating geospatial technologies and data in an effort to prevent, protect against, respond to, and recover from terrorist activity and incidents of national significance. DHS encourages grantees to align geospatial activities with the guidance available on the G&T website at *http://www.ojp.usdoj.gov/odp/grants_hsgp.htm*.

12. Administrative requirements.

12.1 -- 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, and discussions of demographics, transportation, public works, and industrial and public health infrastructures. While this information under Federal control is subject to requests made pursuant to the Freedom of Information Act (FOIA), 5. U.S.C. §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. The applicant is encouraged to consult its 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. The applicant may also consult G&T regarding concerns or questions about the release of information under state and local laws. The grantee 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.

12.2 -- Protected critical infrastructure information (PCII). The PCII Program, established pursuant to the Critical Infrastructure Information Act of 2002 (CII Act), created a new framework, which enables State and local jurisdictions and members of the private sector voluntarily to submit sensitive information regarding critical infrastructure to DHS. The Act also provides statutory protection for voluntarily shared CII from public disclosure and civil litigation. If validated as Protected Critical Infrastructure Information, these documents can only be shared with authorized users who agree to safeguard the information.

PCII accreditation is formal recognition that the covered government entity has the capacity and capability to receive and store PCII. DHS encourages all SAAs to pursue PCII accreditation to cover their state government and attending local government agencies. Accreditation activities include signing an MOA with DHS, appointing a PCII Officer, and implementing a self-inspection program. For additional information about PCII or the accreditation process, please contact the DHS PCII Program Office at *pcii-info@dhs.gov*.

12.3 -- Compliance with federal civil rights laws and regulations. The grantee is required to comply with Federal civil rights laws and regulations. Specifically, the grantee is required to provide assurances as a condition for receipt of Federal from DHS that its programs and activities comply with the following:

- *Title VI of the Civil Rights Act of 1964, as amended, 42. U.S.C. 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. More information can be found at: *http://usinfo.state.gov/usa/infousa/laws/majorlaw/civilr19.htm.*

- *Section 504 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. 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. More information can be found at: *http://www.section508.gov/index.cfm?FuseAction=Content&ID=15.*

- *Title IX of the Education Amendments of 1972, as amended, 20 U.S.C. 1681 et. seq.* – discrimination on the basis of sex is eliminated in any education program or activity receiving Federal financial assistance. More information can be found at: *http://www.usdoj.gov/crt/cor/coord/titleix.htm.*

- *The Age Discrimination Act of 1975, as amended, 20 U.S.C. 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. More information can be found at: *http://www.lawresearchservices.com/firms/admin/act-age.htm.*

Grantees must comply with all regulations, guidelines, and standards adopted under the above statutes. The grantee is 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.

12.4 -- 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. The grantee is 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.lep.gov*.

12.5 -- 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 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.

Further information can be found at the Disability and Emergency Preparedness Resource Center at *http://www.dhs.gov/disabilitypreparedness.*

12.6 -- Compliance with the National Energy Conservation Policy and Energy Policy Acts. In accordance with the FY07 DHS Appropriations Act, all FY07 grant funds must comply with the following two requirements:

- None of the funds made available through the IPP shall be used in contravention of the Federal buildings performance and reporting requirements of Executive Order No. 13123, part 3 of title V of the National Energy Conservation Policy Act (42 USC 8251 et seq), or subtitle A of title I of the Energy Policy Act of 2005 (including the amendments made thereby)**.**

- None of the funds made available through the IPP shall be used in contravention of section 303 of the Energy Policy Act of 1992 (42 USC13212).

12.7 -- National Environmental Policy Act (NEPA). NEPA requires DHS to analyze the possible environmental impacts of each construction project funded by a DHS grant. 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 may be required to provide additional detailed information on the activities to be conducted, locations, sites, possible construction activities, alternatives, and any environmental concerns. Results of the NEPA Compliance Review could result in a project not being approved for funding, the need to perform an Environmental Assessment or draft an Environmental Impact Statement. .

C. Port Application Checklist.

All PSGP applicants must complete the following:

1. **SF-424 Grant Application with Certifications (through *grants.gov*)**
   - Non-Supplanting Certification; assurances; certifications regarding lobbying; debarment, suspension, and other responsibility matters; and drug-free workplace requirement.

2. **DUNS Number (through *grants.gov* form).**

3. **Investment Justification (through *grants.gov* file attachment)**. See Appendix 4.

4. **Detailed Budget (through *grants.gov* file attachment).** See Appendix 5.

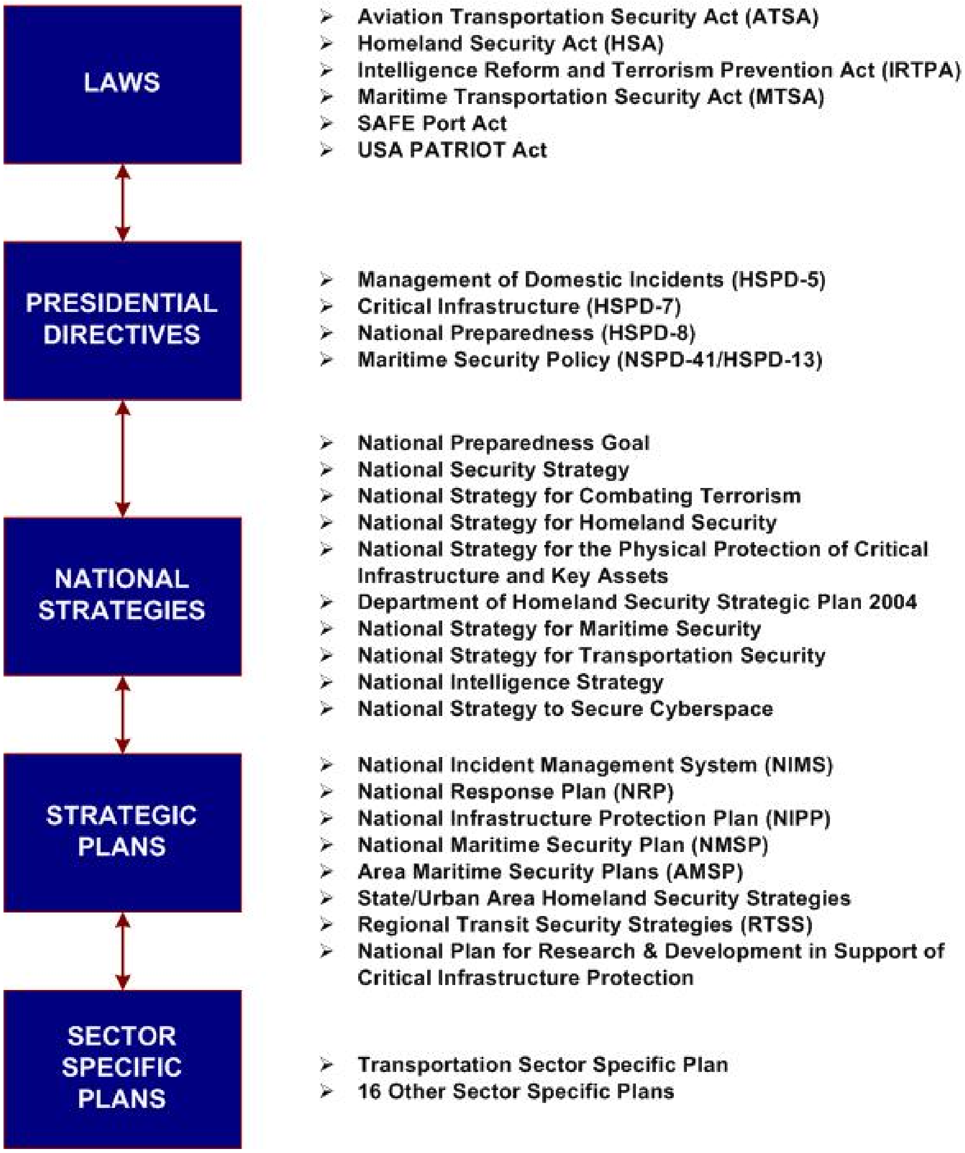
5. **MOU/MOA (through *grants.gov* file attachment).** Applicable for: (1) port authorities or other State and local agencies that provide layered security protection to federally regulated facilities; and (2) consortia composed of local stakeholder groups (i.e., river groups, ports and terminal associations) representing federally regulated ports, terminals, U.S. inspected passenger vessels or ferries that provide layered security protection to federally regulated facilities**.** See Appendix 6.

6. **Accounting System and Financial Capabilities Questionnaire, if applicable (through *grants.gov* file attachment).**

Appendix 1
Alignment of IPP with the National Preparedness Architecture

Figure 1, below, graphically summarizes key elements of the national preparedness architecture. The Infrastructure Protection Program seeks maximum alignment with this architecture.

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



LAWS

- Aviation Transportation Security Act (ATSA)
- Homeland Security Act (HSA)
- Intelligence Reform and Terrorism Prevention Act (IRTPA)
- Maritime Transportation Security Act (MTSA)
- SAFE Port Act
- USA PATRIOT Act

PRESIDENTIAL DIRECTIVES

- Management of Domestic Incidents (HSPD-5)
- Critical Infrastructure (HSPD-7)
- National Preparedness (HSPD-8)
- Maritime Security Policy (NSPD-41/HSPD-13)

NATIONAL STRATEGIES

- National Preparedness Goal
- National Security Strategy
- National Strategy for Combating Terrorism
- National Strategy for Homeland Security
- National Strategy for the Physical Protection of Critical Infrastructure and Key Assets
- Department of Homeland Security Strategic Plan 2004
- National Strategy for Maritime Security
- National Strategy for Transportation Security
- National Intelligence Strategy
- National Strategy to Secure Cyberspace

STRATEGIC PLANS

- National Incident Management System (NIMS)
- National Response Plan (NRP)
- National Infrastructure Protection Plan (NIPP)
- National Maritime Security Plan (NMSP)
- Area Maritime Security Plans (AMSP)
- State/Urban Area Homeland Security Strategies
- Regional Transit Security Strategies (RTSS)
- National Plan for Research & Development in Support of Critical Infrastructure Protection

SECTOR SPECIFIC PLANS

- Transportation Sector Specific Plan
- 16 Other Sector Specific Plans

Appendix 2
PSGP Allowable Expenses

A. Overview.

Specific investments made in support of the funding priorities discussed above generally fall into one of four categories. FY07 PSGP allowable costs are therefore divided into the following four categories:

1. Maritime Domain Awareness
2. IED prevention, protection, response and recovery capabilities
3. Training and exercises
4. Management and administration

The following provides guidance on allowable costs within each of these areas:

1. Maritime Domain Awareness. FY07 PSGP funds may be used for the following types of Maritime Domain Awareness projects:

- Deployment of access control/standardized credentialing systems.
- Deployment of detection and surveillance equipment.
- Development/enhancement of information sharing systems, including equipment (and software) required to receive, transmit, handle, and store classified information.
- Creation/enhancement of maritime community watch programs.
- Construction/enhancements of command and control facilities.
- Enhancement of interoperable communications/asset tracking for sharing terrorism threat information (including ensuring that mechanisms are interoperable with Federal, State, and local agencies).

Applicants 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*.

2. IED Prevention, Protection, Response, Recovery Capabilities. FY07 PSGP funds may be used for the following types of IED prevention, protection, response and recovery capabilities for port areas:

2.1 -- Port Facilities, Including Public Cruise Line and Terminals.

- Explosive agent detection sensors.
- Chemical, biological, or 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 or 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).

2.2 -- Vessels.

- Explosive agent detection sensors.
- Chemical, biological or 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 and standardized credentialing.
- Floating protective barriers.

3. Training and Exercises. FY07 PSGP funds may be used for the following types of training and exercises:

3.1 -- Training*.* Funding used for port security training will be limited to those courses that have been approved by MARAD, the USCG or G&T (including MTSA 109 courses). More information may be obtained at:

- *http://marad.dot.gov/MTSA/MARAD%20Web%20Site%20for%20MTSA%20Course.html*
- *http://www.uscg.mil/stcw/security.pdf*
- *http://www.ojp.usdoj.gov/odp/training.htm*

3.2 -- 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). More information on HSEEP may be found at: *http://www.ojp.usdoj.gov/odp/exercises.htm#hseep*.

Examples of security exercise programs include:

- Area Maritime Security Training and Exercise Program (AMStep): AMStep is the USCG developed mechanism by which AMSCs and Federal Maritime Security Coordinators will continuously improve security preparedness in the port community. It is an integral part and a strategic implementation of the DHS HSEEP for the maritime sector. Rooted in long-standing USCG exercise policy and procedures, AMStep aligns to support the National Preparedness Goal and the National Strategy for Maritime Security. Through a structured approach, AMStep focuses all exercise efforts, both public and private, on improving the AMSPs and individual vessel and facility security plans of the nation's largest seaports.

- Port Security Training and Exercise Program: The Port Security Exercise Training Program (PortSTEP) was established by TSA to develop port security exercise and evaluation services and solutions for maritime and surface industry partners under TSA's guidance and direction. In association with the USCG, TSA has assembled a Program Team to provide strategic support, planning, and analytical and technical services for the delivery of a series of port security training exercises for the transportation security community.

  PortSTEP will provide forty port security training exercises through the applicable AMSCs between August 2005 and October 2007. These include a mix of basic tabletop, advanced tabletop and functional exercises. PortSTEP achieves several performance objectives aimed at improving the intermodal transportation industry's ability to prepare for and contend with a transportation security incident. These objectives are centered on increasing awareness, improving processes, creating partnerships, and delivering port incident training.

  More information on PortSTEP is available at: *http://www.tsa.gov/what_we_do/layers/portstep/editorial_with_table_0061.shtm*.

- National Preparedness for Response Exercise Program: The USCG National Preparedness for Response Exercise Program (PREP) focuses on exercise and evaluation of government area contingency plans and industry spill response plans (oil and hazardous substance). PREP is a coordinated effort of the four Federal agencies with responsibility for oversight of private-sector oil and hazardous substance pollution response preparedness: USCG, the U.S. Environmental Protection Agency, the U.S. Department of Transportation's Research and Special Programs Administration, and the U.S. Department of the Interior's Minerals Management Service. These agencies worked with Federal, State, and local governments, the oil and marine transportation industry, cleanup contractors, and the general public to develop the program. PREP meets the OPA mandate for exercises and represents minimum guidelines for ensuring overall preparedness within the response community. The guidelines, which are reviewed periodically through a public workshop process, outline an exercise program that satisfies the exercise requirements of the four Federal regulatory agencies.

  More information on PREP is available at: *http://www.uscg.mil/hq/nsfweb/download/PREP/MSPREP.PDF*

4. Management and Administration (M&A) Costs. FY07 PSGP funds may be approved for the following management and administrative costs:

- Hiring of full-time or part-time staff, contractors or consultants and M&A expenses related to pre-application submission management activities and application requirements or meeting compliance with grant reporting or data collection requirements, including data calls.

- Development of operating plans for information collection and processing necessary to respond to DHS data calls.

- Travel expenses.

- Meeting-related expenses (for a complete list of allowable meeting-related expenses, please review the OGO *Financial Management Guide* at: *http://www.dhs.gov/xlibrary/assets/Grants_FinancialManagementGuide.pdf .*

B. Other Authorized Expenditure Guidance.

B.1 -- Specific Guidance on Canines.

The USCG 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. ferry systems 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: purchase, 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 or 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 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, the U. S. Police Canine Association or the International Explosive Detection Dog Association may be used to meet this requirement.[10]

- **Submission requirements.** 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.

[10] Training and certification information can be found at: http://www.tsa.gov/public/display?theme=32, http://www.npca.net, http://www.uspcak9.com/html/home.shtml, and http://www.bombdog.org/.

Applicants are encouraged thoroughly to 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 per 33 CFR Part 104.415 detailing the inclusion of a canine explosive detection program into their security measures.

- **Additional resources available for canine costs.** DHS is aware that the financial obligations of a canine explosive detection Program can be burdensome. The PSGP, 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 and Homeland Security Grant Program 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.

B.2 -- Specific Guidance on Employee Identification.

The Transportation Worker Identification Credential (TWIC) is designed to be an open architecture, standards-based system. Port projects that involve new installations or upgrades to access control and credentialing systems, should exhibit compliance with TWIC standards and program specifications. Recipients of grant funding for the implementation of TWIC systems may be requested by the Federal government to apply these systems in a field test of TWIC readers in accordance with the SAFE Port Act. Systems implemented with grant funding may be used by recipients to comply with the TWIC rulemaking requirements.

Recipients may be expected to enter into a cooperative agreement with the Federal government with mutually agreed upon conditions to obtain data and lessons learned from the application of card readers and associated systems. A TWIC rulemaking that will address card reader requirements applied to MTSA-regulated facilities and vessels is expected to be published later this year. Systems implemented with grant funding may be used by recipients to comply with the all TWIC rulemaking requirements.

B.3 -- Specific Guidance on Lighting.

All lighting must meet applicable Occupational Safety and Health Administration requirements.

B.4 -- 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 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.

B.5 -- Specific Guidance on Security Operational and Maintenance Costs.

In accordance with 46 USC Sec. 70107(b)(2), operational and allowable costs include 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. In addition, routine maintenance costs for security monitoring, such as the cost of tapes for recording, are allowable. ***However, business operations and maintenance costs, such as personnel costs and items generally characterized as indirect or "overhead" costs, are unallowable.***

B.6 -- 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 FY07 PSGP. ***However, the development of new risk/vulnerability assessment models and methodologies is unallowable.***

B.7 -- Specific Guidance on Construction.

Section 112(b) of the SAFE Port Act of 2006 places restrictions on the use of PSGP funds for construction projects. It stipulates that funds may not be used to construct buildings or other physical facilities, exception under terms and conditions consistent with the requirements under section 611(j)(8) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121(j)(8) and specifically approved by the Secretary. Costs eligible for funding may not exceed the greater of: (1) $1,000,000 per project; or (2) a greater amount, as approved by the Secretary, which may not exceed 10 percent of the total amount of the grant.

Applicants are advised that grants authorized under the Stafford Act, or that must comply with provisions under the Stafford Act, (including the FY07 PSGP) must follow the standards identified in the Buy American Act. The Buy American Act requires that all materials purchased be produced in the United States, unless such materials are not available, or such a purchase would not be in the public interest. Further, FY07 PSGP grant recipients using funds for construction projects must comply with the Davis-Bacon Act. Additional information on the Davis-Bacon Act is available from the following website: *http://www.dol.gov/esa/programs/dbra/*.

C. Unallowable Costs.

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

- 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 or 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 DHS.
- 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).
- 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" below for further guidance).
- Reimbursement of pre-award security expenses.
- Repair of existing equipment including, but not limited to: fencing, lighting, CCTV or access controls.
- Weapons, including, but not limited to: firearms, ammunition, and weapons affixed to facilities, vessels or other structures.
- 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 and the like.

Appendix 3
Grants.Gov Quick-Start Instructions

DHS participates in the Bush Administration's e-government initiative. As part of that initiative, all IPP applicants must file their applications using the Administration's common electronic "storefront" -- *grants.gov*. Eligible SAAs must apply for funding through this portal, accessible on the Internet at *http://www.grants.gov*.

Application attachments submitted via *grants.gov* must be in one of the following formats: Microsoft Word (*.doc), PDF (*.pdf), or text (*.txt). Use the Catalog of Federal Domestic Assistance (CFDA) number listed in the relevant program guidance section of this document in Grants.gov.

This Appendix is intended to provide guidance on the various steps and activities associated with filing an application using *grants.gov.*

Step 1: Registering.

Registering with *grants.gov* is a one-time process; however, if you are a first time registrant **it could take 3-5 business days to have your registration validated, confirmed, and receive your user name and password**. It is highly recommended you start the registration process as early as possible to prevent delays in submitting your application package to our agency by the deadline specified. While your registration is pending, you may continue with steps 2, 3, and 4 of these instructions. Registration must be complete for you to be able to submit (step 5) and track (step 6) an application.

1. Establishing an e-business point of contact. *Grants.gov* requires an organization to first be registered in the Central Contract Registry (CCR) before beginning the *grants.gov* registration process. If you plan to authorize representatives of your organization to submit grant applications through *grants.gov*, proceed with the following steps. If you plan to submit a grant application yourself and sign grant applications and provide the required certifications and/or assurances necessary to fulfill the requirements of the application process, proceed to DUNS Number and then skip to the Authorized Organization Representative and Individuals section.

Go to *www.grants.gov*, and click on the "Get Started" tab at the top of the screen.

- Click the "e-Business Point of Contact" option and click the "GO" button on the bottom right of the screen. If you have already registered with Grants.gov, you may log in and update your profile from this screen.

- To begin the registration process, click the "Register your Organization [Required]" or "Complete Registration Process [Required]" links. You may print a registration checklist by accessing *www.grants.gov/assets/OrganizationRegCheck.pdf*.

2. DUNS number. You must first request a Data Universal Numbering System (DUNS) number. Click "Step 1. Request a DUNS Number." If you are applying as an individual, please skip to "Authorized Organization Representative and Individuals." If you are applying on behalf of an organization that already has a DUNS number, please proceed to "Step 2. Register with

Central Contractor Registry (CCR)." You may obtain a DUNS number at no cost by calling the dedicated toll-free DUNS number request line at 1–866–705–5711.

3. Central Contractor Registry (CCR). Registering with the CCR, updating or changing your profile could take up to three to five business days to be confirmed and validated. This delay could prevent your application from being submitted by the deadline specified, so you should register or make changes to your profile as early in the process as possible.

Once you have a DUNS number, click on "Step 2. Register with Central Contractor Registry (CCR)." Here you are required to designate an individual as a point of contact. This point of contact is the sole authority for the organization and has the capability of issuing or revoking another individual's authority to submit grant applications through Grants.gov.

A registration worksheet is provided to assist in the CCR registration process at *http://www.ccr.gov.* It is recommended you review the "Tips for registering with the CCR" at the bottom of this template.

- Go to *http://www.ccr.gov* or click on the CCR icon in the middle of the screen to begin the registration process. To see if your organization is already registered, click "Search CCR" at the top left side of the screen. Search entries must be exact to accurately search the database. If your organization is already registered, you can scroll down and see who the e-Business point of contact is for your agency. If your organization is not already registered, return to the CCR home page and click "Start New Registration" at the top left of the screen.

- If you have problems or questions about the CCR registration process, please contact the CCR Assistance Center at 1–888–227–2423.

- Once your registration is complete, you will receive an e-mail with a Trading Partner Identification Number (TPIN) and Marketing Partner Identification Number (MPIN) number. You will need the MPIN number to register with *grants.gov*. If your organization is already registered with the CCR, you will need to obtain the MPIN number from your e-Business POC.

4. Authorize your Organization Representative. Click "Step 3. Authorize your Organization Representative." Follow steps 1-4. You will need your DUNS + 4 digit number and the MPIN number CCR e-mailed to you.

5. Log in as e-Business Point of Contact. You may now go to "Step 4. Log in as e-Business Point of Contact." Here you may authorize or revoke the authority of the Authorized Organization Representative. Once you are logged in, go to Step 2. *Downloading the Application Viewer*, below.

6. Authorized Organization Representative and Individuals. If you plan to submit a grant application as an individual or an Authorized Organization Representative, with authority to sign grant applications and the required certifications and/or assurances necessary to fulfill the requirements of the application process, proceed with the following steps:

- Go to *www.grants.gov* and click on the "Get Started" tab at the top of the screen.

- Click the "Authorized Organization Representative (AOR)" option and click the "GO" button to the bottom right of the screen. If you are applying as an individual, click the "Individuals" option and click the "GO" button to the bottom right of the screen.

- If you have previously registered as an AOR, you may start searching for this grant opportunity from this page. Otherwise, you must complete the first-time registration by clicking "Complete First-Time Registration [Required]." You also may click on "Review Registration Checklist" and print a checklist for the following steps (see *www.grants.gov/assets/AORRegCheck.pdf).*

- Individuals may click the "registration checklist" for help in walking through the registration process.

7. Credential Provider. Once you have entered the registration process, you must register with the credential provider, to safeguard the security of your electronic information. You must have your agency's or individual DUNS + 4 digit number to complete this process. Now, click on "Step 1. Register with a Credential Provider." Enter your DUNS number and click "Register." Once you have entered the required information, click the "Submit" button.

If you should need help with this process, please contact the Credential Provider Customer Service at 1–800–386–6820. It can take up to 24 hours for your credential provider information to synchronize with Grants.gov. Attempting to register with *grants.gov* before the synchronization is complete may be unsuccessful.

8. Grants.gov. After completing the credential provider steps above, click "Step 2. Register with Grants.gov." Enter the same user name and password used when registering with the credential provider. You will then be asked to provide identifying information and your organization's DUNS number. After you have completed the registration process, Grants.gov will notify the e-Business POC for assignment of user privileges.

Complete the "Authorized Organization Representative User Profile" screen and click "Submit." *Note:* Individuals do not need to continue to the "Organizational Approval" step below.

9. Organizational Approval. Prior to submitting a grant application package, you must receive approval to submit on behalf of your organization. This requirement prevents individuals from submitting grant application packages without permission. A notice is automatically sent to your organization's e-Business POC. Then, your e-Business POC approves your request to become an AOR. You may go *to http://www.ccr.gov* to search for your organization and retrieve your e-Business POC contact information.

Once organization approval is complete, you will be able to submit an application and track its status.

Step 2: Downloading the Application Viewer.

You may download the PureEdge Viewer while your registration is in process. You also may download and start completing the application forms in steps 3 and 4 below. This application viewer opens the application package needed to fill out the required forms. The download process can be lengthy if you are accessing the Internet using a dial-up connection.

- From the *grants.gov* home page, select the “Apply for Grants” tab at the top of the screen.

- Under “Apply Step 1: Download a Grant Application Package and Applications Instructions,” click the link for the PureEdge Viewer (*http://www.grants.gov/DownloadViewer*). This window includes information about computer system requirements and instructions for downloading and installation.

If you are a Macintosh user, please read the PureEdge Support for Macintosh white paper available at *www.grants.gov/GrantsGov_UST_Grantee/!SSL!/WebHelp/MacSupportforPureEdge.pdf*.

- Scroll down and click on the link to download the PureEdge Viewer (*www.grants.gov/PEViewer/ICSViewer602_grants.exe*).

- You will be prompted to save the application. Click the “Save” button and the “Save As” window opens. Select the location where you would like to save PureEdge Viewer and click the “Save” button.

- A window appears to show the progress of the download. When the downloading is complete, click to close the dialog box.

- To install the PureEdge Viewer, locate the file on your computer and click to open it. When you are prompted to run the file, click “RUN.” Click “Yes” to the prompt to continue with the installation. The ICS InstallShield Wizard extracts the necessary files and takes you to the “Welcome” page.

- Click “Next” to continue.

- Read the license agreement and click “Yes” to accept the agreement and continue the installation process. This takes you to the “Customer Information” screen.

- Enter a User Name and a Company Name in the designated fields and click “Next.”

- The “Choose Destination Location” window prompts you to select the folder in which PureEdge Viewer will be installed. To save the program in the default folder, click “Next.” To select a different folder, click “Browse.” Select the folder in which you would like to save the program, click on “OK,” then click “Next.”

- The next window prompts you to select a program folder. To save program icons in the default folder, click “Next.” To select a different program folder, type a new folder name or select one from the list of existing folders, then click “Next.” Installation will begin.

- When installation is complete, the “InstallShield Wizard Complete” screen will appear. Click “Finish.” This will launch the “ICS Viewer Help Information” window. Review the information and close the window.

Step 3: Downloading an Application Package.

Once you have downloaded the PureEdge Viewer, you may download and view this application package and solicitation instructions.

- From the *grants.gov* home page, select the “Apply for Grants” tab at the top of the screen.

- Click “Apply Step 1: Download a Grant Application Package and Application Instructions.”

- Enter the CFDA number for this announcement, **97.056**. Then click “Download Package.” This will take you to the “Selected Grants Application for Download” results page.

- To download an application package and its instructions, click the corresponding download link below the “Instructions and Application” column.

- Once you select a grant application, you will be taken to a “Download Opportunity Instructions and Application” screen to confirm that you are downloading the correct application. If you would like to be notified of any changes to this funding opportunity, enter your e-mail address in the corresponding field, then click the “Submit” button.

- After verifying that you have downloaded the correct opportunity information, click the “Download Application Instructions” button. This will open a PDF of this grant solicitation. You may print the solicitation or save it to your computer by clicking either the print icon at the top tool bar or the “File” button on the top tool bar. If you choose to save the file, click on “Save As” and save to the location of your choice.

- Click the “Back” Navigation button to return to the “Download Opportunity Instructions and Application” page. Click the “Download Application Package” button. The application package will open in the PureEdge Viewer.

- Click the “Save” button to save the package on your computer. Because the form is not yet complete, you will see a prompt that one or more fields may be invalid. You will complete these fields in step 4, but for now, select “Yes” to continue. After you click “Yes,” the “Save Form” window will open.

- Save the application package to your desktop until after submission. Select a name and enter it in the “Application Filing Name” field. Once you have submitted the application through *grants.gov*, you may then move your completed application package to the file location of your choice.

- Click the “Save” button. If you choose, you may now close your Internet browser and complete your application package offline by double clicking the icon on your desktop. You do not have to be connected to the Internet to complete the application package in step 4 below.

Step 4: Completing the Application Package.

This application can be completed entirely offline; however, you will need to log in to Grants.gov to submit the application in step 5.

- Locate the application package you saved on your computer. When you open the package, it will be in PureEdge Viewer. You may save your application at any time by clicking on the "Save" button at the top of the screen.

- Enter a name for your application package in the "Application Filing Name" field. This can be a name of your choice.

- Open and complete all the mandatory and optional forms or documents. To complete a form, click to select the form, and then click the "Open" button. When you open a required form, the mandatory fields will be highlighted in yellow. If you enter incomplete information in a mandatory field, you will receive an error message or the field will turn red, indicating a change needs to be made.

- Mandatory forms include the: (1) Application for Federal Assistance (SF-424); (2) Assurances for Non-Construction Programs (SF-424B); and (3) Disclosure of Lobbying Activities (SF-LLL). These forms can also be viewed at *http://apply.grants.gov/agency/FormLinks?family=7*. Other mandatory forms are identified in Section IV.

- When you have completed a form or document, click the "Close Form" button at the top of the page. Your information will automatically be saved.

- Next, click to select the document in the left box entitled "Mandatory Documents." Click the "=>" button to move the form or document to the "Mandatory Completed Documents for Submission" box to the right.

- Some mandatory documents will require you to upload files from your computer. To attach a document, select the corresponding form and click "Open." Click the "Add Mandatory Attachment" button to the left. The "Attach File" box will open. Browse your computer to find where your file is located and click "Open." The name of that file will appear in the yellow field. Once this is complete, if you would like to attach additional files, click on the "Add Optional Attachment" button below the "Add Mandatory Attachment" button.

- An "Attachments" window will open. Click the "Attach" button. Locate the file on your computer that you would like to attach and click the "Open" button. You will return to the "Attach" window. Continue this process until you have attached all the necessary documents. You may attach as many documents as necessary.

- Once you have finished, click the "Done" button. The box next to the "Attach at Least One Optional Other Attachment" will now appear as checked.

- *Note:* the name of these buttons will vary depending on the name of the form you have opened at that time; i.e., Budget Narrative, Other Attachment, and Project Narrative File.

- To exit a form, click the "Close" button. Your information will automatically be saved.

Step 5: Submitting the Application.

Once you have completed all the yellow fields on all the forms and saved the application on your desktop, check the application package for errors. This can be done any time throughout step 4 above and as often as you like.

- When you are ready to submit your final application package, the "Submit" button at the top of your screen will be enabled. This button will not be activated unless all mandatory data fields have been completed. When you are ready to submit your application, click on "Submit." This will take you to a "Summary" screen.

- If your "Submit" button is not activated, then click the "Check Package for Errors" button at the top of the "Grant Application Package" screen. PureEdge Viewer will start with the first form and scan all the yellow fields to make sure they are complete. The program will prompt you to fix one error at a time as it goes through the scan. Once there are no more errors, the system will allow you to submit your application to *grants.gov.*

- Review the application summary. If you wish to make changes at this time, click "Exit Application" to return to the application package, where you can make changes to the forms. To submit the application, click the "Sign and Submit Application" button.

- This will take you to a "Login" screen where you will need to enter the user name and password that you used to register with *grants.gov* in "Step 1: Registering." Enter your user name and password in the corresponding fields and click "Login."

- Once authentication is complete, your application will be submitted. Print this confirmation screen for your records. You will receive an e-mail message to confirm that the application has been successfully uploaded into *grants.gov*. The confirmation e-mail will give you a *grants.gov* tracking number, which you will need to track the status of your application. The confirmation e-mail will go to the e-Business POC; therefore, if you are submitting on behalf of someone else, be sure the e-Business POC is aware of the submission and that a confirmation e-mail will be sent.

- When finished, click the "Close" button.

Step 6: Tracking the Application.

After your application is submitted, you may track its status through *grants.gov*. To do this, go to the *grants.gov* home page at *http://www.grants.gov.* At the very top of the screen, click on the "Applicants" link. Scroll down the "For Applicants" page and click the "Login Here" button. Proceed to login with your user name and password that was used to submit your application package. Click the "Check Application Status" link to the top left of the screen. A list of all the applications you have submitted through *grants.gov* is produced. There four status messages your application can receive in the system:

- **Validated.** This means your application has been scanned for errors. If no errors were found, it validates that your application has successfully been submitted to Grants.gov and is ready for the agency to download your application.

- **Received by Agency.** This means our agency DHS downloaded your application into our electronic Grants Management System (GMS) and your application is going through our validation process to be successfully received on our end.

- **Agency Tracking Number Assigned.** This means our GMS did not find any errors with your package and successfully downloaded your application into our system.

- **Rejected With Errors.** This means your application was either rejected by Grants.gov or GMS due to errors. You will receive an e-mail from *grants.gov* customer support, providing details of the results and the next steps required. Most applications are rejected because: (1) a virus was detected; (2) you are using a user name and password that has not yet been authorized by the organization's e-Business POC; or (3) the DUNS number you entered on the SF-424 form does not match the DUNS number that was registered in the CCR for this organization.

If you experience difficulties at any point during this process, please call the *grants.gov* customer support hotline at 1–800–518–4726.

Appendix 4
Investment Justification

A. Investment Justification Overview.

As part of the application process, applicants must develop a formal Investment Justification that addresses each initiative being proposed for funding. These Investment Justifications must demonstrate how proposed projects address gaps and deficiencies in current programs and capabilities.

Applicants may propose up to three investments within their Investment Justification.

The Investment Justification must demonstrate the ability of the applicant to provide tangible, physical security enhancements consistent with the purpose of the program and guidance provided by DHS. Applicants must ensure that the Investment Justification is consistent with all applicable requirements outlined in this application kit.

B. Investment Justification Template.

PSGP applicants must provide information in the following categories for each proposed Investment:

1. Background;
2. Strategic and program priorities;
3. Impact;
4. Funding and Implementation Plan.

Investment Heading	
Port Area	
Applicant Organization	
Investment Name	
Investment Amount	**$**

I. Background.

Note: This section only needs to be completed once per application, regardless of the number of Investments proposed. The information in this section provides background and context for the Investment(s) requested, but does not represent the evaluation criteria used by DHS for rating individual Investment proposals.

I.A. Provide an overview of the port system in which this Investment will take place.	
Response Type	Narrative
Page Limit	Not to exceed 2 ½ pages
Response Instructions	• Area of Operations: o Identify COTP Zone o Identify eligible port area • Point(s) of contact for organization: o Identify the organization’s Authorizing Official for entering into grant agreement. o Identify the organization’s primary point of contact for management of the project(s). • Ownership or Operation: o 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, or 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): o Identify the specific regulated entities to which you are providing layered protection. o Describe your organization’s specific roles, responsibilities and activities in delivering layered protection. • Infrastructure: o Describe the type, quantity and significance of infrastructure to be protected through the prospective grant. Identify who the infrastructure is owned or operated by, if not by your own organization. • Nature of Operations: o Provide a brief summary of the character and scope of your operations. o Provide specific data/annual statistics that relate to your specific port project (for port applications), terminal project (for terminal applications), waterways, U.S. inspected passenger vessel or ferry projects: ➢ Type and volume of cargo (annual statistics, if applicable) ➢ Type and volume of hazardous materials (annual statistics, if applicable) ➢ Number of passengers (annual statistics, if applicable) ➢ Number of vessels owned (if applicable) *Note: Terminals and vessels cannot rely on aggregated port statistics.* • Other important features: o Describe any other operational issues you deem important to the consideration of your application (e.g., interrelationship of your operations with other eligible high-risk ports, etc.).
Response	

I.B. Describe the applicant’s current and required capabilities.	
Response Type	Narrative
Page Limit	Not to exceed ½ page
Response Instructions	• Describe your organization’s current and required capabilities related to Maritime Domain Awareness. • Describe your organization’s current and required IED prevention, detection, response and recovery capabilities. • Describe your organization’s current and required training and exercise activities.
Response	

I.C. Provide a brief abstract for this Investment.	
Response Type	Narrative
Page Limit	Not to exceed 1 page
Response Instructions	Provide a succinct statement summarizing this Investment.
Response	

II. Strategic and Program Priorities

II.A. Describe how the Investment will address one or more of the National Port Security Priorities.	
Response Type	Narrative
Page Limit	Not to exceed 1 page
Response Instructions	• Describe how, and the extent to which, the proposed investment addresses: o Enhancement of Maritime Domain Awareness o Enhancement of prevention, detection, response and recovery capabilities for: ➢ IED attacks involving small craft or underwater swimmers ➢ IED attacks on passenger and/or vehicle ferries o Training and exercises o TWIC implementation projects o Efforts in support of the national preparedness architecture
Response	

II.B. Describe how the Investment will support priorities outlined in the applicable Area Maritime Security Plan (mandated under the MTSA).

Response Type	Narrative
Page Limit	Not to exceed ½ page
Response Instructions	• Describe how the investment will support priorities outlined in the applicable Area Maritime Security Plan.
Response	

II.C. Describe how the Investment supports any COTP Port-specific security priorities.

Response Type	Narrative
Page Limit	Not to exceed ½ page
Response Instructions	• Describe how the investment supports any port-specific security priorities as set forth by the appropriate COTP.
Response	

II.D. Describe how this Investment will support one or more of the Priorities of the National Preparedness Goal.

Response Type	Narrative
Page Limit	Not to exceed ½ page
Response Instructions	• Explain how this investment will support one or more of the following National Preparedness Priorities: o Expanding regional collaboration; o Implementing the National Incident Management System and the National Response Plan; o Implementing the National Infrastructure Protection Plan; o Strengthening information sharing and collaboration capabilities; o Enhancing interoperable communications capabilities; and, o Strengthening CBRNE detection and response capabilities. *Note: At a minimum, the Investment must support implementation of the National Infrastructure Protection Plan (NIPP).*
Response	

III. Impact

III.A. Describe how the project offers the highest risk reduction potential at the least cost.	
Response Type	Narrative
Page Limit	Not to exceed ½ page
Response Instructions	• Discuss the how the project will reduce risk in a cost effective manner. o Discuss how this investment will reduce risk (e.g., reduce vulnerabilities or mitigate the consequences of an event) by addressing the needs and priorities identified in earlier analysis and review. o Identify the nature of the risk, why you consider it a risk, and how the risk and need are related to show how addressing the need through this investment will also mitigate risk (e.g., reduce vulnerabilities or mitigate the consequences of an event).
Response	

III.B. Describe what the potential homeland security risks of not funding this Investment are.	
Response Type	Narrative
Page Limit	Not to exceed ½ page
Response Instructions	• Consider the risks that already exist and will be more prevalent and/or any new risks that will result if this Investment is not funded and implemented. • Briefly discuss potential outcomes if this risk is not addressed – explain what vulnerabilities will not be reduced or what potential consequences will not be mitigated.
Response	

IV. Funding & Implementation Plan

IV.A. Investment Funding Plan.	
Response Type	Numeric and Narrative
Page Limit	Not to exceed 1 page
Response Instructions	• Complete the chart below to identify the amount of funding you are requesting for this investment only; • Funds should be requested by allowable cost categories (as identified in the FY07 IPP Program Guidance and Application Kit); • Applicants must make funding requests that are reasonable and justified by direct linkages to activities outlined in this particular Investment; and, • Applicants must indicate whether additional funding (non-FY07 PSGP) will be leveraged for this investment. Applicants must provide additional information in question IV.E, indicating the funding source(s) and how those funds will be leveraged. *Note: Investments will be evaluated on the expected impact on security relative to the amount of the investment (i.e., cost effectiveness). An itemized Budget Detail Worksheet and Budget Narrative must also be completed for this investment. See Appendix 5 of this document for a sample format.*
Response	

The following template illustrates how the applicants should indicate the amount of FY07 PSGP funding required for the investment, how these funds will be allocated across the cost elements, and the required cash match:

	FY07 PSGP Request Total	**Cash Match**	**Grand Total**
Maritime Domain Awareness			
Prevention, Protection, Response and Recovery Capabilities			
Training			
Exercises			
TWIC Implementation			
National Preparedness Architecture			
M&A			
Total			

IV.B. Identify up to five (5) potential challenges to the effective implementation of this investment (e.g., stakeholder buy-in, sustainability, aggressive timelines).	
Response Type	Narrative
Page Limit	Not to exceed ½ page
Response Instructions	• For each identified challenge, provide a brief description of how the challenge will be addressed and mitigated, and indicate a probability of occurrence (high, medium, or low); • The response should focus on the implementation only; • Consider the necessary steps and stages that will be required for successful implementation of the Investment; • Identify areas of possible concern or potential pitfalls in terms of Investment implementation; and, • Explain why those areas present the greatest challenge to a successful Investment implementation.
Response	

IV.C. Describe the management team, including roles and responsibilities, that will be accountable for the oversight and implementation of this Investment, and the overall management approach they will apply for the implementation of this investment.	
Response Type	Narrative
Page Limit	Not to exceed ½ page
Response Instructions	• Provide the high-level skill sets (e.g., budget execution, grant administration, geospatial expert, outreach and communication liaison) that members of the management team must possess for the successful implementation and oversight of the investment. • Discuss how those skill sets fulfill the oversight and execution responsibilities for the investment, and how the management roles and responsibilities will be distributed or assigned among the management team. • Explain how the management team members will organize and work together in order to successfully manage the investment.
Response	

IV.D. Discuss funding resources beyond FY07 PSGP that have been identified and will be leveraged to support the implementation and sustainment of this investment.	
Response Type	Narrative
Page Limit	Not to exceed ½ page
Response Instructions	• In addition to the required cash match, discuss other funding sources (e.g., non-PSGP grant programs, public or private agreements, future fiscal year grants) that you plan on utilizing for the implementation and/or continued sustainment of this investment; • If no other funding resources have been identified beyond the required cash match, or if none are necessary, provide rationale as to why the requested FY07 PSGP funding is sufficient for the implementation and sustainment of this investment.
Response	

IV.E. Provide a high-level timeline, milestones and dates, for the implementation of this Investment. Possible areas for inclusion are: stakeholder engagement, planning, major acquisitions or purchases, training, exercises, and process/policy updates. Up to 10 milestones may be provided.	
Response Type	Narrative
Page Limit	Not to exceed 1 page
Response Instructions	• Only include major milestones that are critical to the success of the Investment; • While up to 10 milestones may be provided, applicants should only list as many milestones as necessary; • Milestones are for this discrete Investment – those that are covered by the requested FY07 PSGP funds and will be completed over the 36-month grant period; • Milestones should be kept to high-level, major tasks that will need to occur; • Identify the planned start date associated with the identified milestone. The start date should reflect the date at which the earliest action will be taken to start achieving the milestone; • Identify the planned completion date when all actions related to the milestone will be completed and overall milestone outcome is met; and, • List any relevant information that will be critical to the successful completion of the milestone (such as those examples listed in the question text above).
Response	

IV.F. Describe the planned duration for this overall Investment. Discuss your long-term sustainability plans for the investment after your FY07 PSGP funds have been expended, if applicable.	
Response Type	Narrative
Page Limit	Not to exceed ½ page
Response Instructions	• Give the expected total life-span for this investment if fully implemented and sustained through completion. • Consider how this Investment will be sustained and funded after FY07 PSGP funds are expended, if applicable. • Include information about resource needs (e.g., personnel, processes, and tools), as well as critical governance needs. • List critical milestones that are outside of the FY07 PSGP grant period, and how those milestones will be met with the identified funding and resources.
Response	

IV.G. Describe the technical implementation plan for this investment. Discuss the innovativeness of the solution proposed.	
Response Type	Narrative
Page Limit	Not to exceed ½ page
Response Instructions	• Define the vision, goals, and objectives for the risk reduction. Summarize how the proposed investment will fit into the overall effort to meet the critical infrastructure security priorities (including integration into existing security protocols). • Describe the specific needs and/or resource limitations that need to be addressed. • Identify specific equipment needs (e.g., number of facility cameras, number of security lights, amount of security fencing, etc.) and other details for training, awareness, exercises and other programs, if applicable (e.g., number of people to be trained, length of training, type of training, number of printed materials, number of agencies and staff members involved in exercise planning, execution, and review). • Describe progress made on the security project this Investment will be completing, if applicable. • Reference use of prior year grant funds, if applicable.
Response	

C. Investment Justification Submission and File Naming Convention.

Investment Justifications must be submitted with the grant application as a file attachment within *grants.gov*. Applicants must use the following file naming convention when submitting required documents as part of the FY07 PSGP:

- COTP Zone Abbreviation_Port Area_Name of Applicant_ IJ Number
  (Example: Hous_Galveston_XYZ Oil_IJ#1)

Appendix 5

Sample Budget Detail Worksheet

OMB Approval No. 1121-0188

Purpose. The Budget Detail Worksheet may be used as a guide to assist applicants in the preparation of the budget and budget narrative. You may submit the budget and budget narrative using this form or in the format of your choice (plain sheets, your own form, or a variation of this form). However, all required information (including the budget narrative) must be provided. Any category of expense not applicable to your budget may be deleted.

A. Personnel. List each position by title and name of employee, if available. Show the annual salary rate and the percentage of time to be devoted to the project. Compensation paid for employees engaged in grant activities must be consistent with that paid for similar work within the applicant organization.

Name/Position	Computation	Cost

Note: Personnel costs are only allowable for direct management and administration of the grant award, i.e., preparation of mandatory post-award reports.

TOTAL __________

B. Fringe Benefits. Fringe benefits should be based on actual known costs or an established formula. Fringe benefits are for the personnel listed in budget category (A) and only for the percentage of time devoted to the project. Fringe benefits on overtime hours are limited to FICA, Workman's Compensation and Unemployment Compensation.

Name/Position	Computation	Cost

TOTAL __________

Total Personnel & Fringe Benefits __________

C. Travel. Itemize travel expenses of project personnel by purpose (e.g., staff to training, field interviews, advisory group meeting, etc.). Show the basis of computation (e.g., six people to 3-day training at $X airfare, $X lodging, $X subsistence). In training projects, travel and meals for trainees should be listed separately. Show the number of trainees and unit costs involved. Identify the location of travel, if known. Indicate source of Travel Policies applied, Applicant or Federal Travel Regulations.

Purpose of Travel	Location	Item	Computation	Cost

TOTAL __________

D. Equipment. List non-expendable items that are to be purchased. Non-expendable equipment is tangible property having a useful life of more than two years. (Note: Organization's own capitalization policy and threshold amount for classification of equipment may be used). Expendable items should be included either in the "Supplies" category or in the "Other" category. Applicants should analyze the cost benefits of purchasing versus leasing equipment, especially high cost items and those subject to rapid technical advances. Rented or leased equipment costs should be listed in the "Contractual" category. Explain how the equipment is necessary for the success of the project. Attach a narrative describing the procurement method to be used.

Item	Computation	Cost

Budget Narrative: Provide a narrative budget justification for each of the budget items identified.

TOTAL _________

E. Supplies. List items by type (office supplies, postage, training materials, copying paper, and other expendable items such as books, hand held tape recorders) and show the basis for computation. (Note: Organization's own capitalization policy and threshold amount for classification of supplies may be used). Generally, supplies include any materials that are expendable or consumed during the course of the project.

Supply Items	Computation	Cost

TOTAL _________

F. Consultants/Contracts. Indicate whether applicant's formal, written Procurement Policy or the Federal Acquisition Regulations are followed.

Consultant Fees: For each consultant enter the name, if known, service to be provided, hourly or daily fee (8-hour day), and estimated time on the project.

Name of Consultant	Service Provided	Computation	Cost

Budget Narrative: Provide a narrative budget justification for each of the budget items identified.

Subtotal ___________

Consultant Expenses: List all expenses to be paid from the grant to the individual consultant in addition to their fees (i.e., travel, meals, lodging, etc.)

Item	Location	Computation	Cost

Budget Narrative: Provide a narrative budget justification for each of the budget items identified.

Subtotal __________

Contracts: Provide a description of the product or services to be procured by contract and an estimate of the cost. Applicants are encouraged to promote free and open competition in awarding contracts. A separate justification must be provided for sole source contracts in excess of $100,000.

Item	**Cost**

Budget Narrative: Provide a narrative budget justification for each of the budget items identified.

Subtotal ________

TOTAL __________

G. Other Costs. List items (e.g., rent, reproduction, telephone, janitorial or security services, and investigative or confidential funds) by major type and the basis of the computation. For example, provide the square footage and the cost per square foot for rent, and provide a monthly rental cost and how many months to rent.

Description	**Computation**	**Cost**

Budget Narrative: Provide a narrative budget justification for each of the budget items identified.

Important Note: If applicable to the project, construction costs should be included in this section of the Budget Detail Worksheet.

TOTAL _________

H. Indirect Costs. Indirect costs are allowed only if the applicant has a Federally approved indirect cost rate. A copy of the rate approval, (a fully executed, negotiated agreement), must be attached. If the applicant does not have an approved rate, one can be requested by contacting the applicant's cognizant Federal agency, which will review all documentation and approve a rate for the applicant organization, or if the applicant's accounting system permits, costs may be allocated in the direct costs categories.

Description	**Computation**	**Cost**

TOTAL _________

Budget Summary - When you have completed the budget worksheet, transfer the totals for each category to the spaces below. Compute the total direct costs and the total project costs. Indicate the amount of Federal funds requested and the amount of non-Federal funds that will support the project.

Budget Category	Federal Amount	Non-Federal Amount
A. Personnel	___________	___________
B. Fringe Benefits	___________	___________
C. Travel	___________	___________
D. Equipment	___________	___________
E. Supplies	___________	___________
F. Consultants/Contracts	___________	___________
G. Other	___________	___________
Total Direct Costs	___________	___________
H. Indirect Costs	___________	___________
*** TOTAL PROJECT COSTS**	___________	___________

Federal Request ___________

Non-Federal Amount ___________

Detailed Budget Submission and File Naming Convention.

The Detailed Budget must be submitted with the grant application as a file attachment within *grants.gov*. Applicants must use the following file naming convention when submitting required documents as part of the FY07 PSGP:

- COTP Zone Abbreviation_Port Area_Name of Applicant_IJ Number_Budget
  (Example: Hous_Galveston_XYZ Oil_IJ#1_Budget)

Appendix 6
MOU/MOA Consortia or Association Guidance

A. Requirement for State or Local Agencies and for Consortia or Associations.

Entities that provide layered security to MTSA regulated facilities are eligible applicants. In addition, the layered protection provided must be addressed in the regulated entities' security plan. A copy of a Memorandum of Understanding (MOU) or a Memorandum of Agreement (MOA) between those identified entities will be required prior to funding, and must include an acknowledgement of the layered security and roles and responsibility of all entities involved. The MOU/MOA must address the following points:

- The nature of the security that the applicant agrees to supply to the regulated facility (waterside surveillance, increased screening, etc)
- The roles and responsibilities of the facility and the applicant during different MARSEC levels.
- An acknowledgement by the facility that the applicant is part of their facility security plan.

If the applicant is mentioned as a provider of layered security under the port's Area Maritime Security Plan, in lieu of an MOA/MOU, acknowledgement from the Area Maritime Security Committee (AMSC) members, or a letter from the Federal Maritime Security Coordinator validating this status, will be acceptable. *In addition, MOA/MOUs submitted in previous PSGP award rounds will be acceptable, provided the activity covered also addresses the capability being requested through the FY07 PSGP.*

B. Sample MOU/MOA Template.

Memorandum of Understanding / Agreement
Between [provider of layered security] and [recipient of layered security]
Regarding [provider of layered security's] use of port security grant program funds

1. PARTIES. The parties to this Agreement are the [Provider of Layered Security] and the [Recipient of Layered Security].

2. AUTHORITY. This Agreement is authorized under the provisions of [applicable Area Maritime Security Committee authorities and/or other authorities].

3. PURPOSE. The purpose of this Agreement is to set forth terms by which [Provider of Layered Security]shall expend Port Security Grant Program project funding in providing layered security to [Recipient of Layered Security]. Under requested FY07 PSGP grant, the [Provider of Layered Security] must provide layered security to [Recipient of Layered Security] consistent with the approach described in an approved grant application.

4. RESPONSIBILITIES: The security roles and responsibilities of each party are understood as follows:

(1). [Recipient of Layered Security]

Roles and responsibilities in providing its own security at each MARSEC level

(2) [Provider of Layered Security]

- An acknowledgement by the facility that the applicant is part of their facility security plan.
- The nature of the security that the applicant agrees to supply to the regulated facility (waterside surveillance, increased screening, etc).
- Roles and responsibilities in providing security to [Recipient of Layered Security] at each MARSEC level.

5. POINTS OF CONTACT. [Identify the POCs for all applicable organizations under the Agreement; including addresses and phone numbers (fax number, e-mail, or internet addresses can also be included).]

6. OTHER PROVISIONS. Nothing in this Agreement is intended to conflict with current laws or regulations of [applicable state] or [applicable local Government). If a term of this agreement is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this agreement shall remain in full force and effect.

7. EFFECTIVE DATE. The terms of this agreement will become effective on (EFFECTIVE DATE).

8. MODIFICATION. This agreement may be modified upon the mutual written consent of the parties.

9. TERMINATION. The terms of this agreement, as modified with the consent of both parties, will remain in effect until the grant end dates for an approved grant. Either party upon [NUMBER] days written notice to the other party may terminate this agreement.

APPROVED BY:

____________________________	______________________________
Organization and Title	Signature
(Date)	(Date)

C. Submitting the MOU/MOA.

If applicable, the MOU/MOA for state or local law enforcement agencies and/or consortia providing layered protection to regulated entities must be submitted with the grant application as a file attachment within *grants.gov*.

- COTP Zone Abbreviation_Port Area_Name of Applicant_MOU
  (Example: Hous_Galveston_Harris County_MOU)

Appendix 7
Award and Reporting Requirements

A. Grant Award and Obligation of Funds.

Upon approval of an application, the grant will be awarded to the grant recipient. The date that this is done is the "award date." The signed award document with special conditions must be returned to:

Office of Justice Programs,
Attn: Control Desk – G&T Award
810 7th Street, N.W., 5th Floor
Washington, DC 20531.

An obligation is defined in the *Office of Grant Operations (OGO) Financial Management Guide* as a legally binding liability under a grant, sub-grant, and/or contract determinable sums for services or goods incurred during the grant period.

The period of performance is 36 months from the date of award. Any unobligated funds will be deobligated by DHS at the end of this period. Extensions to the period of performance will be considered only through formal requests to G&T with specific and compelling justifications why an extension is required.

B. Post Award Instructions.

G&T's OGO will provide fiscal support and oversight of the grant programs, while the OJP Office of the Comptroller will continue to provide support for grant payments. The following is provided as a guide for the administration of awards. Additional details and requirements may be provided to the grantee in conjunction with finalizing an award.

1. Review award and special conditions document. Notification of award approval is made by e-mail through the OJP Grants Management System (GMS). Once an award has been approved, a notice is sent to the e-mail address of the individual who filed the application, as well as to the authorized grantee official. Carefully read the award and any special conditions or other attachments.

If you agree with the terms and conditions, the authorized official should sign and date both the original and the copy of the award document page in Block 19. You should maintain a copy and return the original signed documents to:

Office of Justice Programs
Attn: Control Desk - G&T Award
810 Seventh Street, N.W., 5th Floor
Washington, DC 20531

If you do not agree with the terms and conditions, contact the awarding G&T Program Manager as noted in the award package.

2. Read the guidelines. Read and become familiar with the "*OGO Financial Management Guide*" which is available at 1-866-9ASKOGO or online at: *http://www.dhs.gov/xlibrary/assets/Grants_FinancialManagementGuide.pdf.*

3. Complete and return ACH form. The Automated Clearing House (ACH) Vendor/ Miscellaneous Payment Enrollment Form (refer to Step 3 attachment) is used to arrange direct deposit of funds into your designated bank account.

4. Access to payment systems. OJP uses the Phone Activated Paperless System (PAPRS) to request funds. Grantees will receive a letter with the award package containing their PIN to access the system and Grant ID information.

5. Reporting Requirements. Reporting requirements must be met during the life of the grant (refer to the *OGO Financial Management Guide* and the specific program guidance for a full explanation of these requirements, special conditions and any applicable exceptions). The payment system contains edits that will prevent access to funds if reporting requirements are not met on a timely basis. Refer to Step 5 attachments for forms, due date information, and instructions.

6. Questions about your award? A reference sheet is provided containing frequently asked financial questions and answers. Questions regarding grant payments should be addressed to the OJP Office of the Comptroller at 1-800-458-0786 or email at: *askoc@ojp.usdoj.gov.* Questions regarding all other financial/administrative issues should be addressed to the OGO Information Line at 1-866-9ASKOGO (927-5646) or email at: *ask-ogo@dhs.gov.*

Note: If you have any questions about GMS, need to establish a GMS account, or require technical assistance with accessing your award, contact the GMS Hotline at 1-888-549-9901.

C. Drawdown and Expenditure of Funds.

Following acceptance of the grant award and release of any special conditions withholding funds, the grantee can drawdown and expend grant funds through the Phone Activated Paperless System (PAPRS). There is a limited pool of grantees that may use the Automated Standard Application for Payments (ASAP).

In support of continuing efforts 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 of each month. Grant recipients 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 October, the last day to request (draw down) payments was October 24, 2006. Payments requested after that date were processed when the regular schedule resumed on November 1, 2006. A similar schedule will follow at the end of each month.

Grant recipients 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 draw down funds up to 120 days prior to expenditure/

disbursement. G&T 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, at: *http://www.access.gpo.gov/nara/cfr/waisidx_04/28cfrv2 _04.html* and the Uniform Rule 28 CFR Part 70, Uniform Administrative Requirements for Grants and Agreements (Including Sub-awards) with Institutions of Higher Education, Hospitals and other Non-profit Organizations, at: *http://www.access.gpo.gov/nara/cfr/ waisidx_04/28cfrv2_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

The sub-grantee may keep interest amounts up to $100 per year for administrative expenses for all Federal grants combined. Please consult the OGO *Financial Management Guide* or the applicable OMB Circular for additional guidance. Although advance drawdown requests may be made, State grantees remain subject to the interest requirements of the Cash Management Improvement Act (CMIA) and its implementing regulations at 31 C.F.R. Part 205. Interest under CMIA will accrue from the time Federal funds are credited to a State account until the time the State pays out the funds or transfers the funds to a sub-grantee.

Note: Although advance drawdown requests may be made, State grantees remain subject to the interest requirements of the Cash Management Improvement Act (CMIA) and its implementing regulations at 31 CFR Part 205. Interest under CMIA will accrue from the time Federal funds are credited to a State account until the time the State pays out the funds for program purposes.

D. Reporting Requirements.

1. Financial Status Report (FSR) -- required quarterly. 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 draw downs will be withheld if these reports are delinquent.

FSRs must be filed online through the Internet at: *https://grants.ojp.usdoj.gov.* Forms and instructions can be found at: *http://www.ojp.usdoj.gov/forms.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*
- OMB Circular A-122, *Cost Principles for Non-Profit Organizations,* at: *http://www.whitehouse.gov/omb/circulars/index.html*

For FY07 awards, grant and sub-grant recipients should refer to the OGO Financial Guide. All awards from FY05 and earlier are still governed by the OJP Financial Guide, available at: *http://www.ojp.usdoj.gov/FinGuide.* OGO can be contacted at 1-866-9ASKOGO or by email at: *ask-OGO@dhs.gov.*

Required submission: Financial Status Report (FSR) SF-269a (due quarterly).

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 though 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.ojp.usdoj.gov*. Forms and instructions can be found at: *http://www.ojp.usdoj.gov/forms.htm.*

Required submission: CAPR (due semiannually).

3. Exercise Evaluation and Improvement. Exercises implemented with grant funds should be threat- and performance-based and should evaluate performance of critical prevention and response tasks required to respond to the exercise scenario. Guidance on conducting exercise evaluations and implementing improvement is defined in the *Homeland Security Exercise and Evaluation Program (HSEEP) Volume II: Exercise Evaluation and Improvement* located at: *http://www.ojp.usdoj.gov/G&T/docs/HSEEPv2.pdf.* Grant recipients must report on scheduled exercises and ensure that an AAR and IP are prepared for each exercise conducted with G&T support (grant funds or direct support) and submitted to G&T within 60 days following completion of the exercise.

The AAR documents the performance of exercise related tasks and makes recommendations for improvements. The Improvement Plan (IP) outlines the actions that the exercising jurisdiction(s) plans to take to address recommendations contained in the AAR. Generally the IP, with at least initial action steps, should be included in the final AAR. G&T is establishing a national database to facilitate the scheduling of exercises, the submission of the AAR/IPs and the tracking of IP implementation. Guidance on the development of AARs and IPs is provided in Volume II of the HSEEP manuals.

Required submissions: AARs and IPs (as applicable).

4. 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 U.S. General Accountability Office, *Government Auditing Standards*, located at: *http://www.gao.gov/govaud/ybk01.htm*, and *OMB Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations*, located at: *http://www.whitehouse.gov/omb/circulars/a133/a133.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 FY07 IPP 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.

The State shall require that sub-grantees comply with the audit requirements set forth in *OMB Circular A-133*. Recipients are responsible for ensuring that sub-recipient audit reports are received and for resolving any audit findings.

5. Federal Funding Accountability and Transparency Act. While there are no State and Urban Area requirements in FY07, the Federal Funding Accountability and Transparency Act of 2006 may affect State and Urban Area reporting requirements in future years. The Act requires the Federal government to create a publicly searchable online database of Federal grant recipients by January 1, 2008 with an expansion to include sub-grantee information by January 1, 2009

6. National Preparedness Reporting Compliance. The Government Performance and Results Act (GPRA) requires that the Department collect and report performance information on all programs. For grant programs, the prioritized Investment Justifications and their associated milestones provide an important tool for assessing grant performance and complying with these national preparedness reporting requirements. G&T will work with grantees to develop tools and processes to support this requirement. DHS anticipates using this information to inform future-year grant program funding decisions.

7. National Assessment of State and Local Preparedness. HSPD-8 calls for an assessment of national preparedness. Furthermore, the FY07 DHS Appropriations Act requires a comprehensive national assessment of State and local preparedness in FY07. Additional guidance will be provided during the grant period regarding these requirements. DHS will strive to ensure reporting requirements support State and local level performance management requirements, where applicable. Congress also requires a Federal Preparedness Report on the Nation's level of preparedness for all hazards, including natural disasters, acts of terrorism, and other man-made disasters, including an estimate of the amount of Federal, State, local, and Tribal expenditures required to attain the National Preparedness Priorities by October 4, 2007, and annually thereafter.

8. Catastrophic Resource Report. The Department is also required to develop and submit an annual Catastrophic Resource Report which estimates the resources of DHS and other Federal agencies needed for and devoted specifically to developing the capabilities of Federal, State, local, and Tribal governments necessary to respond to a catastrophic incident. This requirement includes an estimate of State, local and Tribal government catastrophic incident preparedness.

9. State Preparedness Report. Congress requires that States receiving DHS-administered Federal preparedness assistance shall submit a State Preparedness Report to the Department on the State's level of preparedness by January 4, 2008, and annually thereafter. The report shall include (A) an assessment of State compliance with the national preparedness system, NIMS, the NRP, and other related plans and strategies; (B) an assessment of current capability levels and a description of target capability levels; and (C) an assessment of resource needs to meet the National Preparedness Priorities, including an estimate of the amount of expenditures required to attain the Priorities and the extent to which the use of Federal assistance during the preceding fiscal year achieved the Priorities.

E. Monitoring.

Grant recipients will be monitored periodically by DHS staff, both programmatically and financially, to ensure that the project goals, objectives, performance requirements, timelines, milestone completion, budgets and other related program criteria are being met. Monitoring will be accomplished through a combination of office-based reviews and on-site monitoring visits. Monitoring will involve the review and analysis of the financial, programmatic, performance 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, maintaining of adequate financial records, and refunding expenditures disallowed by audits.

F. Grant Close-Out Process.

Within 90 days after the end of the award period, grantees must submit a final FSR and final CAPR detailing all accomplishments throughout the project. After 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 deobligated, and address the requirement of maintaining the grant records for three years from the date of the final FSR. After the financial information is received and approved by OGO, the grant will be identified as "Closed by the Office of Grant Operations."

Required submissions: (1) final SF-269a, due 90 days from end of grant period; and (2) final CAPR/BSIR, due 90 days from the end of the grant period.

Appendix 8
Additional Resources

This Appendix describes several resources that may help applicants in completing a TSPG application.

1. Centralized Scheduling & 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 of CBRNE, agro-terrorism, 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.

The CSID can be contacted at 1-800-368-6498 or *askcsid@dhs.gov*. CSID hours of operation are from 8:00 am–6:00 pm (EST), Monday-Friday.

2. Office of Grant Operations (OGO). G&T's Office of Grant Operations will provide fiscal support, including pre- and post-award administration and technical assistance, 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 1-866-9ASKOGO or *ask-ogo@dhs.gov*. All payment related questions should be referred to the Office of Justice Programs/Office of the Comptroller (OJP/OC) Customer Service at 1-800-458-0786 or *askoc@ojp.usdoj.gov*. All grant and sub-grant recipients should refer to the OGO *Financial Management Guide*.

3. GSA's Cooperative Purchasing Program. The U.S. General Services Administration (GSA) offers an efficient and effective procurement tool for State and local governments to purchase information technology products and services to fulfill homeland security and other needs. The Cooperative Purchasing Program allows for State and local governments to purchase from Schedule 70 (the Information Technology Schedule) and the Consolidated Schedule (containing IT Special Item Numbers) only. Under this program, State and local governments have access to over 3,000 GSA Schedule contractors who have voluntarily modified their contracts to participate in the Cooperative Purchasing program.

State and local governments can find eligible contractors on GSA's website, *www.gsaelibrary.gsa.gov*, *d*enoted with a COOP PURCH symbol. Assistance is available from GSA at the local and national level. For assistance at the local level visit *www.gsa.gov/csd* to find the point of contact in your area and for assistance at the national level, contact Patricia Reed *at* *patricia.reed@gsa.gov, 213-534-0094. More information is available at www.gsa.gov/cooperativepurchasing.*

4. Exercise Direct Support. DHS has engaged multiple contractors with significant experience in designing, conducting, and evaluating exercises to provide support to States and local jurisdictions in accordance with State Homeland Security Strategies and HSEEP. Contract support is available to help States conduct an Exercise Plan Workshop, develop a Multi-year Exercise Plan and build or enhance the capacity of States and local jurisdictions to design, develop, conduct, and evaluate effective exercises.

In FY07, states may receive direct support for three exercises: one T&EPW, one discussion-based exercise, and one operations-based exercise. While states are allowed to submit as many direct support applications as they choose, they are strongly encouraged to give careful thought to which exercises will require the additional assistance that will be provided through the Direct Support program. Exercises involving cross-border or mass-gathering issues will be counted against the number of direct-support exercises being provided to states.

Applications for direct support are available at http://hseep.dhs.gov and are reviewed on a monthly basis. HSEEP offers several tools and resources to help design, develop, conduct and evaluate exercises.