



**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

KEY CHANGES IN FY 2007 .....	i
CONTENTS .....	ii
INTRODUCTION.....	1
PART I. AVAILABLE FUNDING AND ELIGIBLE APPLICANTS.....	5
PART II. APPLICATION EVALUATION PROCESS.....	10
PART III. PROGRAM REQUIREMENTS .....	14
APPENDIX 1. ALIGNMENT OF IPP WITH THE NATIONAL PREPAREDNESS ARCHITECTURE.....	21
APPENDIX 2. PSGP ALLOWABLE EXPENSES.....	22
APPENDIX 3. <i>GRANTS.GOV</i> QUICK-START INSTRUCTIONS.....	29
APPENDIX 4. INVESTMENT JUSTIFICATION.....	37
APPENDIX 5. SAMPLE BUDGET DETAIL WORKSHEET.....	46
APPENDIX 6. MOU/MOA CONSORTIA OR ASSOCIATION GUIDANCE.....	50
APPENDIX 7. AWARD AND REPORTING REQUIREMENTS .....	52
APPENDIX 8. ADDITIONAL RESOURCES .....	58

## 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).<sup>1</sup> 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

---

<sup>1</sup> 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.<sup>2</sup> 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.

---

<sup>2</sup> 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.<sup>3</sup>

#### **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.

---

<sup>3</sup> 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
<b>TOTAL</b>	<b>\$201,170,000</b>

*Applicants are encouraged not to request more than two times the average percentage of IPP funds received annually from FY03 through FY06.<sup>4</sup>* 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

<sup>4</sup> 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<sup>5</sup> 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.

---

<sup>5</sup> 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<sup>6</sup> 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**

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

<sup>6</sup> 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.

U.S. DEPARTMENT OF HOMELAND SECURITY – PORT SECURITY GRANT PROGRAM

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

U.S. DEPARTMENT OF HOMELAND SECURITY – PORT SECURITY GRANT PROGRAM

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
<b>Total FY07 PSGP Allocation</b>			<b>\$201,170,000</b>

## 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.<sup>7</sup>

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.

---

<sup>7</sup> 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.<sup>8</sup>

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.

---

<sup>8</sup> 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.<sup>9</sup>
  - **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>.

---

<sup>9</sup> 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](http://www.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](http://www.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](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\\_hsqp.htm](http://www.ojp.usdoj.gov/odp/grants_hsqp.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.