

**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](mailto: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.

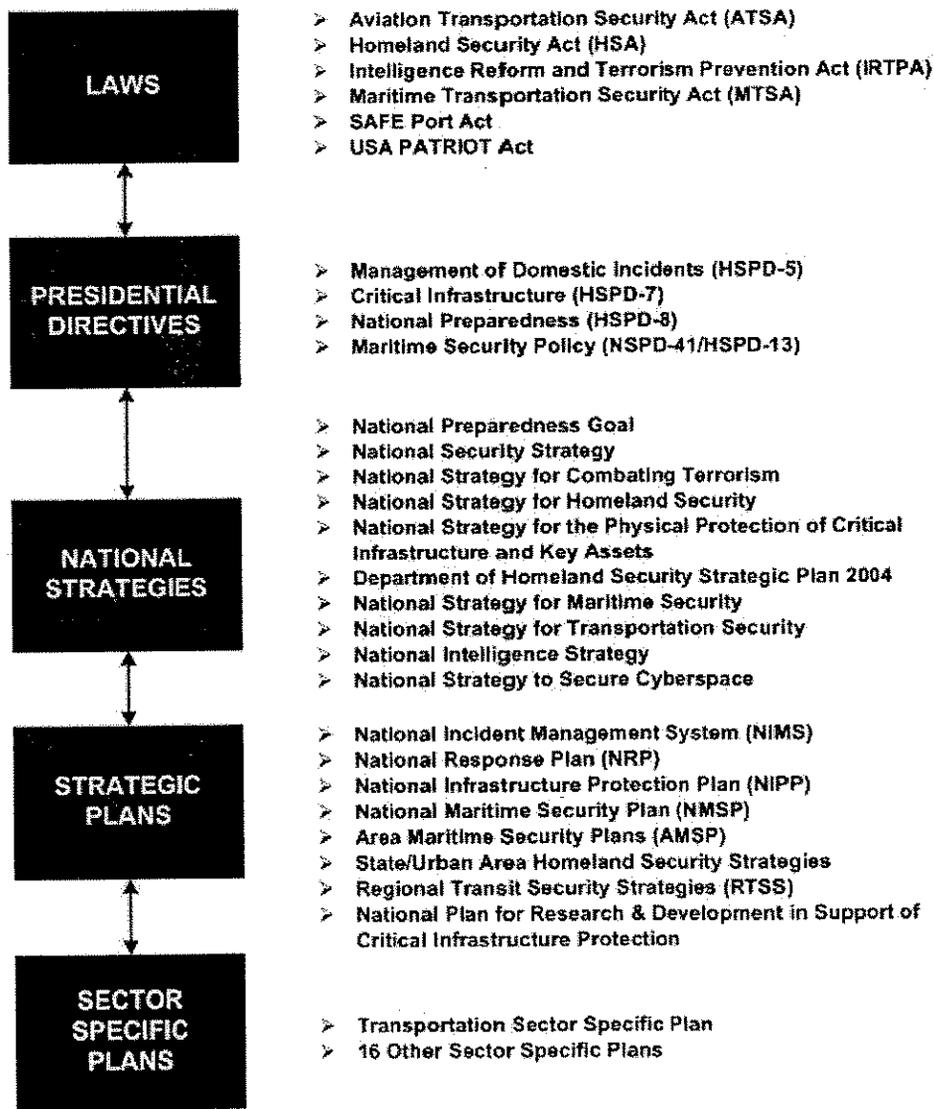
*All PSGP applicants must complete the following:*

- 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**



## 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](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](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.<sup>10</sup>
- **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.

---

<sup>10</sup> 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](http://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/OrganizationReqCheck.pdf](http://www.grants.gov/assets/OrganizationReqCheck.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](http://www.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](http://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/AORReqCheck.pdf](http://www.grants.gov/assets/AORReqCheck.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](http://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](http://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.