U.S. DEPARTMENT OF HOMELAND SECURITY

Fiscal Year 2007
INFRASTRUCTURE PROTECTION PROGRAM:

BUFFER ZONE PROTECTION 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.

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 final review of applications. Some of the IPP, such as this Buffer Zone Protection Program, 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 to 36 months. New federal legislation requires compliance with federal energy policy laws and certain other administrative requirements.

As with other DHS infrastructure grant programs, the largest portion of the Buffer Zone Protection Program grant dollars will 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 this grant guidance document and must have read and accepted all program guidance as binding.

CONTENTS

INTRODUCTION

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

The vast bulk of America's critical infrastructure is owned and/or operated by State, local and private sector partners. The funds provided by the BZPP are provided to increase the preparedness capabilities of responsible jurisdictions in communities surrounding high-priority critical infrastructure and key resource (CI/KR) assets through allowable planning and equipment acquisition.

The purpose of this package is to provide: (1) an overview of the BZPP; 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.

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 jurisdictions 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 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 Infrastructure Protection Plan and its forthcoming sector-specific plans. The National Preparedness Goal is an all-

[1] The IPP's other components include grants targeted for intracity rail and bus transit (including Amtrak and ferry systems), marine ports, intercity bus companies, and the trucking industry's Highway Watch® program.

hazards vision regarding the nation's four core preparedness objectives: prevent, protect, respond and recover from terrorist attacks and catastrophic natural disasters.

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

DHS expects its critical infrastructure partners – including recipients of IPP grants – to be familiar with this federal 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 FY07 BZPP, as a component of the IPP, provides funds to increase the preparedness capabilities of responsible jurisdictions in communities surrounding high-priority CI/KR assets through planning and equipment acquisition.

The BZPP assists responsible jurisdictions in building effective prevention and protection capabilities that will make it more difficult for terrorists to conduct site surveillance or launch attacks within the immediate vicinity of selected CI/KR assets. These capabilities are enumerated in Buffer Zone Plans (BZPs) that:

- Identify significant assets at the site(s) that may be targeted by terrorists for attack.
- Identify specific threats and vulnerabilities associated with the site(s) and its significant assets.
- Develop an appropriate buffer zone extending outward from the facility in which preventive and protective measures can be employed to make it more difficult for terrorists to conduct site surveillance or launch attacks.
- Identify all applicable law enforcement jurisdictions and other Federal, State, and local agencies having a role in the prevention of, protection against, and response to terrorist threats or attacks specific to the CI/KR site(s) and

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

appropriate points of contact within these organizations.

- Evaluate the capabilities of the responsible jurisdictions with respect to terrorism prevention and response.
- Identify specific planning, equipment, training, and/or exercise requirements to better enable responsible jurisdictions to mitigate threats and vulnerabilities of the site(s) and its buffer zone.

In developing and implementing the BZPs, security and preparedness officials at all levels should seek opportunities to coordinate and leverage funding from multiple sources, including Federal, State, and local resources.

C. Allowable Expenses.

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

1. Planning
2. Equipment acquisitions
3. Management and administration

Appendix 2 provides additional detail about each of these three allowable expense categories, as well as a section that identifies several specifically unallowed cost items.

PART I.
AVAILABLE FUNDING AND ELIGIBLE APPLICANTS

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

A. Available Funding.

In FY07, the total amount of funds distributed under the BZPP will be $48.5 million. This is up from $47.9 million distributed in FY06.

B. Selection of Eligible Applicants.

The risk methodology for the IPP programs is consistent across the modes and is linked to the risk methodology used to determine eligibility for the core DHS State and local grant programs. Leveraging information collected through State data calls and Federal Sector Specific Agency (SSA) input, DHS has made substantial gains in the accuracy of data incorporated into its analyses to yield a better understanding of the relative risk to specific CI/KR sites. This improvement provides DHS with the ability to focus the allocation of BZPP resources to those jurisdictions responsible for the highest risk sites.

All BZPP sites have been selected prior to the grant announcements based on the risk of the individual sites themselves. Therefore, BZPP funding allocated to any given State or territory is entirely a function of the number, type, and character of pre-identified higher-risk sites within their respective jurisdictions; there are no discretionary sites.[3] Several States have sites that are close in proximity. DHS will work closely with these States and provide supplemental guidance within the FY07 BZPP timelines to ensure coordinated planning.

Through the FY07 BZPP, DHS continues to build on its cross-sector baseline knowledge of CI/KR and the systematic approach initiated in FY06 to focus sufficient resources to reduce the risk associated with the highest priority CI/KR assets across certain targeted sectors. These include:

- Higher consequence chemical facilities
- Nuclear power plants
- Higher consequence liquefied natural gas facilities
- Higher consequence liquefied petroleum gas facilities

[3] In the course of closing gaps at sites specifically identified by DHS in the 2007 BZPP, if a State has any residual grant funding remaining from the allocation provided upon completion of all necessary activities to develop a BZP at the DHS selected site(s), the State may redirect the residual funds to another CI/KR site, subject to justification and DHS final approval.

- Higher consequence dams
- Critical telecommunications facilities
- Critical banking and finance facilities
- Critical water systems
- Select identified regions with multiple high-risk CI/KR sites[4]

B.1 -- Characterization of CI/KR Tiers.

DHS has established a set of consequence thresholds to identify sites that have the potential to be considered CI/KR *Tier 1* assets, and thus eligible for higher funding levels. To be considered CI/KR *Tier 1*, the asset or system must be documented to have the potential, if successfully destroyed or disrupted through terrorist attack, to cause major national or regional impacts.[5] These include combinations of the following characteristics:

- Nationally significant loss of life
- Severe cascading economic impacts
- Mass evacuations with relocation for an extended period of time
- Impact to a city, region, or sector of the economy due to contamination, destruction, or disruption of vital services to the public
- Severe national security impacts

DHS worked with the SSAs to establish sector-by-sector criteria for CI/KR *Tier 2* assets that would identify those CI/KR sites having inherently greater consequence potential than other assets within their sectors. DHS worked with States to identify assets that met these criteria. Sites nominated by the States through this process were subsequently validated by the Federal SSAs.

CI/KR sites that may otherwise meet the criteria identified above, but are not being addressed through the FY07 BZPP, include:

- Sites that have been sufficiently addressed through prior grants
- Sites eligible for funding through other HSGP and/or IPP funding that more directly address risks associated with the specific site
- Sites, particularly those associated with systems, whose risks DHS has determined may be more appropriately addressed in future program years

This year's BZPP work builds upon the program plan and methodology in place last year. In essence, we prioritized the list of Tier I and Tier II assets, and we are systematically applying available funds to work through the list of assets this program can support. Based upon the results of DHS's prioritization work with State and local colleagues, the following States, Territories, and the District of Columbia are eligible to participate in, and receive funding under, the FY07 BZPP. The specific sites and their

[4] This includes identified dense-urban environments and regional clusters of similar asset types.
[5] DHS is increasingly leveraging a Common Risk Model to identify and compare risks across all sectors. This model is maturing and it is expected that new risks will be identified as more assets and systems are assessed.

locations are sensitive and DHS has directly contacted each jurisdiction with information regarding the identity and location as well as funding amounts of the selected high-risk sites in their area.

Table 1. FY07 BZPP Funding Allocations

States / Territories	Total FY 2007 BZPP Funding
Alabama	$770,000
Arizona	$2,077,500
Arkansas	$577,500
California	$4,695,000
Connecticut	$192,500
Delaware	$192,500
District of Columbia	$1,500,000
Florida	$2,310,000
Georgia	$962,500
Hawaii	$385,000
Idaho	$385,000
Illinois	$1,540,000
Indiana	$1,347,500
Iowa	$192,500
Kansas	$385,000
Kentucky	$962,500
Louisiana	$3,080,000
Maine	$192,500
Maryland	$770,000
Massachusetts	$577,500
Michigan	$1,155,000
Minnesota	$962,500
Mississippi	$192,500
Missouri	$1,155,000
Montana	$192,500
Nebraska	$385,000
Nevada	$385,000
New Hampshire	$385,000
New Jersey	$1,540,000
New York	$4,425,000
North Carolina	$770,000
Ohio	$2,310,000
Oklahoma	$385,000
Oregon	$192,500
Pennsylvania	$1,655,000
Puerto Rico	$192,500
Rhode Island	$692,500
South Carolina	$770,000
Tennessee	$1,847,500
Texas	$2,810,000
Utah	$577,500
Virginia	$770,000
Washington	$577,500
West Virginia	$500,000
Wisconsin	$385,000
Wyoming	$192,500
Total	**$48,500,000**

C. Eligible Applicants and Role of State Administrative Agencies (SAAs).

The Governor of each State has designated an SAA to apply for and administer the funds under BZPP.[6] The SAA is the only agency eligible to apply for BZPP funds and is responsible for obligating BZPP funds to the appropriate responsible units of government or other designated recipients.[7] The SAA must coordinate all BZPP activities with the respective State Homeland Security Advisor (HSA). Each State shall make no less than ***95 percent*** of the total grant program amount available to the responsible unit of government within 60 days of the approval notification for the Vulnerability Reduction Purchase Plan (VRPP). The VRPP identifies a spending plan to protect given infrastructure assets. In includes the planning activities and equipment necessary to implement the BZP. Details about the VRPP content and format have been provided to SAAs that administer this program.

[6] As defined in the Homeland Security Act of 2002, the term ''State'' means "any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States."

[7] As defined in the Conference Report accompanying the Department of Homeland Security Appropriations Act of 2007, the term "local unit of government" means "any county, city, village, town, district, borough, parish, port authority, transit authority, intercity rail provider, commuter rail system, freight rail provider, water district, regional planning commission, council of government, Indian tribe with jurisdiction over Indian country, authorized Tribal organization, Alaska Native village, independent authority, special district, or other political subdivision of any State."

PART II.
APPLICATION EVALUATION PROCESS

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

A. Overview -- Application Deadline and BZP Guidance.

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 budgets and application process requirements -- described herein.

A.1 -- Development of the BZP and VRPP.

- Site vulnerability and jurisdiction capability assessments are critical elements of the BZPP process. Jurisdictions are expected to evaluate their relevant prevention and protection capabilities in accordance with the Target Capabilities List (TCL), and conduct, or leverage, existing vulnerability assessments of the specific infrastructure site, including the zone outside the perimeter of the potential target. The assessment process must include coordination with security management, where possible, and consideration of security and safety measures already in place at the facility.

- The responsible jurisdictions are required to share these assessments with the Preparedness Directorate so that DHS may better prioritize preventive and protective programs, as they may be relevant to emerging and specific threats.

- Upon completion of these assessments, the jurisdictions must complete the BZP template in coordination with the State for each identified CI/KR site. Additionally, the development of the BZP must be coordinated with the following entities, as applicable:

  - Urban Area Working Groups (UAWGs)
  - Area Maritime Security Committees (AMSCs)

  The BZP template serves as a useful tool that can be integrated to support CI/KR protection program planning efforts across all sectors. The BZP will serve as the basis to identify the required planning and equipment necessary to address identified vulnerabilities and/or capability gaps.

- Upon completion of the BZP, the jurisdictions must complete a VRPP. The VRPP identifies a spending plan, including the planning activities and equipment necessary to implement the BZP.

A.2 -- Submission of the BZP and VRPP.

- The BZP and VRPP must be provided to the SAA, to coordinate BZPP implementation with existing State and/or Urban Area Homeland Security Strategies and programs, implementation of the NIPP, and related HSGP and CI/KR protection program funding.

- The SAA, in coordination with the HSA, must certify that each BZP and the requested resources/activities in the associated VRPP support and/or complement:

  - Statewide efforts to develop a CI/KR protection program and associated capabilities, as directed in the NIPP
  - The implementation of the NIPP national priority, as reflected within each respective State's Homeland Security Strategy.

- Upon certification, the SAA must submit the BZP and VRPP for each site to DHS for approval by **November 30, 2007**. ***If States fail to submit all BZPP materials by this date, funds may be deobligated by G&T.***

- The BZPs and VRPPs must be submitted electronically via *the G&T Secure Portal* located at: *https://odp.esportals.com/.* The *G&T Secure Portal* will contain a FY07 BZPP folder for each State.

- The certified BZPs and VRPPs will be reviewed by DHS to ensure that BZPP programmatic and planning activities and requested equipment are coordinated with overall Statewide CI/KR protection efforts, and related strategic goals and objectives.

- Upon review and approval of the BZPs and VRPPs by DHS, the SAA will be notified via email and the responsible jurisdiction(s) may drawdown and expend grant funds obligated by the SAA for implementation of the BZP.

- If the BZP and/or VRPP are incomplete or do not meet program requirements, the SAA may be requested to re-submit program materials or provide additional information.

- All email correspondence between the grantee and DHS related to the application, submission, approval, and/or revision of BZPs and VRPPs must carbon copy the *BZPP@dhs.gov* email address. The actual BZPs and VRPPs themselves should never be sent via email.

- Funds under the FY07 BZPP may not be obligated, drawn down, or expended by the State to the responsible jurisdiction of the identified site until all of the above steps have been completed by the jurisdiction and approved by DHS.

B. BZPP Coordination Requirements.

B.1 -- Private Sector Coordination. Critical infrastructure is largely privately-owned and operated. Enhancing public/private partnerships will leverage private sector initiatives, resources, and capabilities, as permitted by applicable laws and regulations.

B.2 -- Urban Area Working Group Coordination. Each identified Urban Areas Security Initiative (UASI) geographical area is governed by a UAWG. The UAWG is composed of multi-discipline and multi-jurisdictional representatives and is responsible for coordinating development and implementation of all UASI program initiatives, Urban Area Homeland Security Strategy development, and any direct services that are delivered by G&T. Responsible jurisdictions must coordinate the development and implementation of the BZP and VRPP with any UAWGs, as applicable to their geographic area, to ensure all programs, plans, and requested resources are coordinated and leveraged across the region.

C. BZPP Technical Assistance Visits and Workshops.

The DHS Office of Infrastructure Protection (IP) Risk Management Division (RMD) also provides a range of services to BZPP grantees and subgrantees. This includes BZP workshops, which train local law enforcement and other prevention personnel on the BZP process. RMD also provides on-site technical assistance for officials needing technical support in developing and/or implementing BZPs. For more information, please contact: *Frank.Waller1@dhs.gov*.

PART III.
PROGRAM REQUIREMENTS

A. General Program Requirements.

The applicable SAA's will be responsible for administration of the FY07 BZPP.

The period of performance for the FY07 BZPP is **36 months** from the date of award. Any un-obligated funds will be de-obligated by G&T at the end of this period. Extensions to the period of performance will be considered only through formal requests to G&T with specific and compelling justifications as to why an extension is warranted.

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 BZPP 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*.

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

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

   While registration with *grants.gov* and the CCR is a one-time process, new applicants are strongly encouraged to complete their registrations at least 10 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 "*Buffer Zone Protection Program."* The CFDA number is 97.078. When completing the on-line application, applicants should identify their submissions as new, non-construction applications.

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

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

7. **Standard financial requirements.**

7.1 -- 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.

7.2 -- 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.

7.3 -- 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.*

7.4 -- 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*.

8. Technology requirements.

8.1 -- 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 Extensible Markup Language (XML) for all IPP awards. Further information about the required use of NIEM specifications and guidelines is available at *http://www.niem.gov*.

8.2 -- Geospatial guidance. Geospatial technologies capture, store, analyze, transmit, and/or display location-based information (i.e., information that can be linked to a latitude and longitude). State, local, and industry partners are increasingly incorporating geospatial technologies and data in an effort to prevent, protect against, respond to, and recover from terrorist activity and incidents of national significance. DHS encourages grantees to align geospatial activities with the guidance available on the G&T website at *http://www.ojp.usdoj.gov/odp/grants_hsgp.htm.*

9. Administrative requirements.

9.1 -- 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.

9.2 -- 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 PCII, 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*.

9.3 -- 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 197*2, *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.

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. Additional information about the civil rights laws and regulations mentioned above may be found at *http://www.dhs.gov/xabout/structure/editorial_0371.shtm*.

9.4 -- 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, see *http://www.lep.gov*.

9.5 -- Integrating individuals with disabilities into emergency planning. Executive Order No. 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.*

9.6 -- 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 USC 13212).

9.7 -- 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, possible alternatives, and any environmental concerns that may exist. Results of the NEPA Compliance Review could result in a project not being approved for DHS funding, the need to perform an Environmental Assessment or draft an Environmental Impact Statement.

C. BZPP Application Checklist.

All BZPP applicants must complete the following:

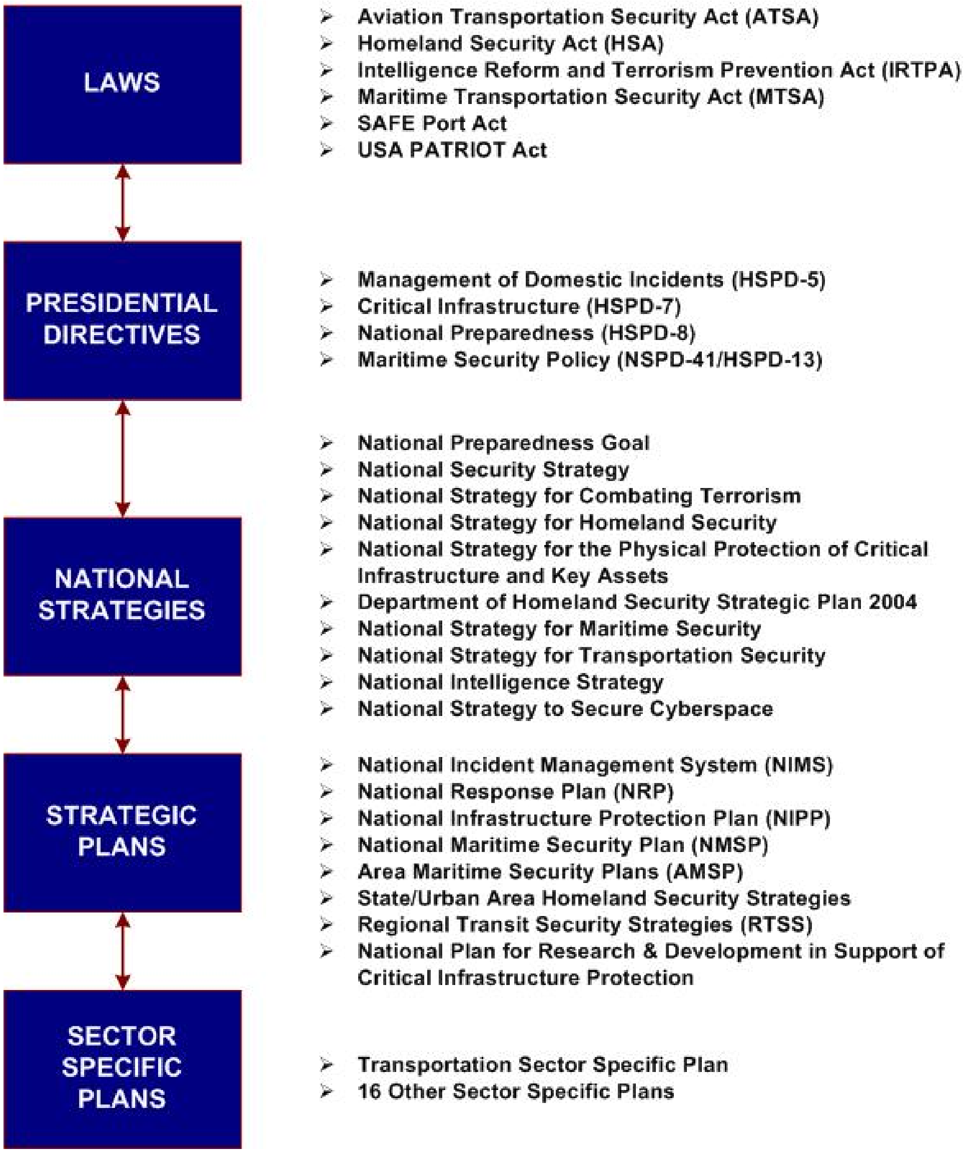
1. **SF-424 Grant Application with Certifications (through *grants.gov*)**
   - Non-supplanting certification
   - Assurances
   - Certifications regarding lobbying; debarment, suspension, and other responsibility matters; and drug-free workplace requirement

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

Appendix 1
Alignment of IPP with the National Preparedness Architecture

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

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



LAWS

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

PRESIDENTIAL DIRECTIVES

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

NATIONAL STRATEGIES

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

STRATEGIC PLANS

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

SECTOR SPECIFIC PLANS

- Transportation Sector Specific Plan
- 16 Other Sector Specific Plans

Appendix 2
BZPP Allowable Expenses

A. Overview.

FY07 BZPP allowable costs are divided into the following three categories:

1. Planning
2. Equipment acquisitions
3. Management and administration

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

This section provides guidance on the types of expenditures that are allowable under the FY07 BZPP. Grantees are encouraged to contact their G&T Preparedness Officer regarding authorized and unauthorized expenditures.

1. Planning. Planning activities are central to the implementation of the BZPP. Accordingly, responsible jurisdictions may use up to 15 percent of BZPP programmatic funds to support multi-discipline planning activities.

FY07 BZPP funds may be used for a range of homeland security and critical infrastructure planning activities, such as:

1.1 -- Developing and implementing homeland security and CI/KR support programs and adopting DHS national initiatives limited to the following:

- Implementing the National Preparedness Goal, as it relates to implementation of the NIPP, and sector specific plans.
- Building or enhancing preventive radiological and nuclear detection programs.
- Modifying existing incident management and Emergency Operating Plans (EOPs) to ensure proper alignment with the NRP and the NIMS coordinating structures, processes, and protocols.
- Establishing or enhancing mutual aid agreements or MOUs to ensure cooperation with respect to CI/KR protection.
- Developing communications and interoperability protocols and solutions with the BZPP infrastructure site.
- Developing or enhancing radiological and nuclear alarm resolution reachback relationships across local, State and Federal partners.
- Developing or updating resource inventory assets in accordance to typed resource definitions issued by the NIMS Integration Center.
- Designing State and local geospatial data systems.

1.2 -- Developing related terrorism prevention and protection programs including:

- Planning to enhance preventive detection capabilities, security and population evacuation in the vicinity of specified CI/KR during heightened alerts, during terrorist incidents, and/or to support mitigation efforts.

- Multi-discipline preparation and integration across the homeland security community.
- Developing or enhancing radiological and nuclear alarm resolution protocols and procedures.
- Developing and planning for information/intelligence sharing groups and/or fusion centers.
- Acquiring systems allowing connectivity to Federal data networks, such as the National Crime Information Center (NCIC) and Integrated Automated Fingerprint Identification System (IAFIS), as appropriate.

1.3 -- Developing and enhancing plans and protocols, limited to:

- Developing or enhancing EOPs and operating procedures.
- Developing terrorism prevention/deterrence plans.
- Developing or enhancing cyber security plans.
- Developing or enhancing cyber risk mitigation plans.
- Developing public/private sector partnership emergency response, assessment, and resource sharing plans.
- Developing or updating local or regional communications plans.
- Developing plans to support and assist special needs jurisdictions, such as port authorities and rail and mass transit agencies.
- Developing and/or updating plans and protocols to support evacuation planning efforts.

The VRPP must clearly show how any funds identified for planning activities support the implementation of prevention and protection capabilities of the responsible jurisdiction, as they are related to the identified CI/KR site(s).

2. Equipment. Select Authorized Equipment List (AEL) categories are eligible for funding (see Table 2 below). The allowable equipment categories are listed on the web-based AEL on the Responder Knowledge Base (RKB), at *http://www.rkb.mipt.org*. DHS-adopted standards can be found at *http://www.dhs.gov/xfrstresp/standards/ editorial_0420.shtm*.

The FY07 AEL is housed on the Responder Knowledge Base along with separate listings for the Authorized Equipment List and the Standardized Equipment List (SEL). In some cases, items on the SEL are not allowable under FY07 BZPP, or will not be eligible for purchase unless specific conditions are met. Unless otherwise specified, maintenance costs/contracts for authorized equipment purchased using FY07 BZPP funding or acquired through G&T's Homeland Defense Equipment Reuse Program are allowable.

Table 2. BZPP Allowable Equipment Categories

#	Category Title
[2]	Explosive Device Mitigation and Remediation Equipment
[3]	CBRNE Operational Search and Rescue Equipment*
[4]	Information Technology
[5]	Cyber Security Enhancement Equipment
[6]	Interoperable Communications Equipment
[7]	Detection Equipment
[10]	Power Equipment
[13]	Terrorism Incident Prevention Equipment

#	Category Title
[14]	Physical Security Enhancement Equipment
[15]	Inspection and Screening Systems
[16]	Agricultural Terrorism Prevention, Response, and Mitigation Equipment
[20.3]	Intervention Equipment - Equipment, Fingerprint Processing, and Identification*
[21]	Other Authorized Equipment

***** Only select sub-categories within AEL Category 3 and 20 are eligible for FY07 BZPP funding. These sections include: 3.1.6, 3.2.2, 3.2.3, 3.2.4, and 20.3.

Other specialized equipment not listed in the above AEL categories may be requested by the responsible jurisdiction, as approved by the State. The responsible jurisdiction must provide a justification describing and/or identifying the following:

- The reason the equipment is requested.
- The target capabilities, per the TCL, the request will support and/or enhance.
- How other grant funding has been considered, or may be applied, to support the request.
- How the requested equipment will support the development and/or implementation of prevention and/or protection capabilities, per the TCL, within the responsible jurisdiction, as identified by the BZP.
- How the equipment will directly address a threat, vulnerability, and/or consequence directly related to the identified FY07 BZPP site and its responsible jurisdiction, as identified by the BZP (i.e., PPE for a jurisdiction responsible for a chemical facility).
- Address a specific threat, vulnerability, and/or consequence directly related to a heightened alert period, as related to the site and/or its sector.

Unless otherwise noted, equipment must be certified that it meets required regulatory and/or DHS-adopted standards to be eligible for purchase using these funds. In addition, agencies must have all necessary certifications and licenses for the requested equipment, as appropriate, prior to the request.

3. Management and Administrative (M&A) Costs. No more than 5 percent of the total State award under FY07 BZPP may be used for M&A by either the State or subgrantee in aggregate.

The following M&A costs are allowable only within the period of performance of the grant program:

- Hiring of full-time or part-time staff or contractors/consultants:
  - To assist with the management and/or administration of the FY07 BZPP.
  - To assist with the coordination and implementation requirements of the FY07 BZPP.
- Hiring of full-time or part-time staff or contractors/consultants and expenses related to:
  - Meeting compliance with reporting and data collection requirements, including data call requests.
  - FY07 BZPP pre-application submission management activities and application requirements.
- Travel expenses.
- Meeting-related expenses.
- Other allowable M&A expenses:

- Acquisition of authorized office equipment, including personal computers, laptop computers, printers, LCD projectors, and other equipment or software which may be required to support the implementation of the BZP or VRPP.
- Recurring fees/charges associated with certain equipment, such as cell phones, faxes, etc.
- Leasing and/or renting of space for newly hired personnel to administer the FY07 BZPP.

B. Unallowable Costs.

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

- **Hiring of Public Safety Personnel.** FY07 BZPP funds may not be used to support the hiring of sworn public safety officers for the purposes of fulfilling traditional public safety duties or to supplant traditional public safety positions and responsibilities.

- **Construction and Renovation.** Construction and renovation is prohibited under the FY07 BZPP.

- **General-use Expenditures.** Expenditures for items such as general-use software (word processing, spreadsheet, graphics, etc), general-use computers and related equipment (other than for allowable M&A activities, or otherwise associated preparedness functions), general-use vehicles, licensing fees, weapons, weapons systems and accessories, and ammunition are prohibited.

- **Federal Improvement.** Funds may not be used for the improvement of Federal buildings or for other activities that solely benefit the Federal government.

- **Training and Exercise Activities.** Any resulting training or exercise requirements identified through the BZPP may not be funded with FY07 BZPP funds, but may be funded through other overarching homeland security grant programs (i.e. State Homeland Security Program, Urban Areas Security Initiative, and/or Law Enforcement Terrorism Prevention Program funds) in accordance with their stipulated authorized expenditures.

  Additionally, the following initiatives and costs are considered **<u>ineligible</u>** for award consideration:

  - Initiatives that do not address the implementation of programs/initiatives to build preparedness capabilities directed at identified facilities and/or the surrounding communities.

  - The development of risk/vulnerability assessment models.

  - Initiatives that fund risk or vulnerability security assessments or the development of BZPs and/or VRPPs.

  - Initiatives in which Federal agencies are the beneficiary or that enhance Federal property.

- Initiatives which study technology development.
- Proof-of-concept initiatives.
- Initiatives that duplicate capabilities being provided by the Federal government.
- Operating expenses.
- Reimbursement of pre-award security expenses.
- Other indirect costs.

Any other activities unrelated to the implementation of the BZPP, items not in accordance with the AEL, or previously identified as ineligible within this guidance, are not an allowable cost.

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 CCR before beginning the *grants.gov* registration process. If you plan to authorize representatives of your organization to submit grant applications through *grants.gov*, proceed with the following steps. If you plan to submit a grant application yourself and sign grant applications and provide the required certifications and/or assurances necessary to fulfill the requirements of the application process, proceed to DUNS Number and then skip to the Authorized Organization Representative and Individuals section.

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

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

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

2. DUNS number. You must first request a Data Universal Numbering System 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. Registering with the CCR, updating or changing your profile could take up to three to five business days to be confirmed and validated. This delay could prevent your application from being submitted by the deadline specified, so you should register or make changes to your profile as early in the process as possible.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 2: Downloading the Application Viewer.

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

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

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

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

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

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

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

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

- Click "Next" to continue.

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

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

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

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

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

Step 3: Downloading an Application Package.

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

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

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

- Enter the CFDA number for this announcement, **97.078**. 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
Award and Reporting Requirements

A. Grant Award and Obligation of Funds.

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

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

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

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

B. Post Award Instructions.

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

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

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

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

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

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

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

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

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

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

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

C. Drawdown and Expenditure of Funds.

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

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

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

Grant recipients should request funds based upon immediate disbursement requirements. Funds will not be paid in a lump sum, but rather disbursed over time as project costs are incurred or anticipated. Recipients should time their drawdown requests to ensure that Federal cash on hand is the minimum needed for disbursements to be made immediately or within a few days. Grantees may elect to draw down funds up to 120 days prior to expenditure/ disbursement. DHS strongly encourages recipients to draw down funds as close to expenditure as possible to avoid accruing interest.

Funds received by grantees must be placed in an interest-bearing account and are subject to the rules outlined in the Uniform Rule 28 CFR Part 66, Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments, at: *http://www.access.gpo.gov/nara/cfr/waisidx_04/28cfrv2_04.html* and the Uniform Rule 28 CFR Part 70, Uniform Administrative Requirements for Grants and Agreements (Including Sub-awards) with Institutions of Higher Education, Hospitals and other Non-profit Organizations, at: *http://www.access.gpo.gov/nara/cfr/ waisidx_04/28cfrv2_04.html.* These guidelines state that entities are required to promptly, but at least quarterly, remit interest earned on advances to:

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

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

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

D. Reporting Requirements.

1. Financial Status Report (FSR) -- required quarterly. Obligations and expenditures must be reported to G&T on a quarterly basis through the FSR, which is due within 30 days of the end of each calendar quarter (e.g., for the quarter ending March 31, FSR is due on April 30). Please note that this is a change from previous fiscal years. A report must be submitted for every quarter the award is active, including partial calendar quarters, as well as for periods where no grant activity occurs. Future awards and fund draw downs will be withheld if these reports are delinquent.

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

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

- OMB Circular A-102, *Grants and Cooperative Agreements with State and Local Governments*, at: *http://www.whitehouse.gov/omb/circulars/index.html*

- OMB Circular A-87, *Cost Principles for State, Local, and Indian Tribal Governments,* at: *http://www.whitehouse.gov/omb/circulars/index.html*

- OMB Circular A-110, *Uniform Administrative Requirements for Grants and Other Agreements with Institutions of Higher Education, Hospitals and Other Non-Profit Organizations*, at *http://www.whitehouse.gov/omb/circulars/index.html*

- OMB Circular A-21, *Cost Principles for Educational Institutions,* at: *http://www.whitehouse.gov/omb/circulars/index.html*

- OMB Circular A-122, *Cost Principles for Non-Profit Organizations,* at: *http://www.whitehouse.gov/omb/circulars/index.html*

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

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

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

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

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

Required submission: CAPR (due semiannually).

3. Financial and Compliance Audit Report. Recipients that expend $500,000 or more of Federal funds during their fiscal year are required to submit an organization-wide financial and compliance audit report. The audit must be performed in accordance with the U.S. General Accountability Office, *Government Auditing Standards*, located at: *http://www.gao.gov/govaud/ybk01.htm*, and *OMB Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations*, located at: *http://www.whitehouse.gov/omb/circulars/a133/a133.html.* Audit reports are currently due to the Federal Audit Clearinghouse no later than nine months after the end of the recipient's fiscal year. In addition, the Secretary of Homeland Security and the Comptroller General of the United States shall have access to any books, documents, and records of recipients of FY07 IPP assistance for audit and examination purposes, provided that, in the opinion of the Secretary of Homeland Security or the Comptroller General, these documents are related to the receipt or use of such assistance. The grantee will also give the sponsoring agency or the Comptroller General, through any authorized representative, access to, and the right to examine all records, books, papers or documents related to the grant.

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

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

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

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

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

8. State Preparedness Report. Congress requires that States receiving DHS-administered Federal preparedness assistance shall submit a State Preparedness Report to the Department on the State's level of preparedness by January 4, 2008, and annually thereafter. The report shall include (1) an assessment of State compliance with the national preparedness system, NIMS, the NRP, and other related plans and strategies; (2) an assessment of current capability levels and a description of target capability levels; and (3) an assessment of resource needs to meet the National Preparedness Priorities, including an estimate of the amount of expenditures required to attain the Priorities and the extent to which the use of Federal assistance during the preceding fiscal year achieved the Priorities.

E. Monitoring.

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

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

F. Grant Close-Out Process.

Within 90 days after the end of the award period, SAAs must submit a final FSR and final CAPR detailing all accomplishments throughout the project. After these reports have been reviewed and approved by G&T, a Grant Adjustment Notice (GAN) will be completed to close out the grant. The GAN will indicate the project as being closed, list any remaining funds that will be deobligated, and address the requirement of maintaining the grant records for three years from the date of the final FSR. After the financial information is received and approved by OGO, the grant will be identified as “Closed by the Office of Grant Operations.”

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

Appendix 5
Additional Resources

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

1. Centralized Scheduling & Information Desk (CSID) Help Line. The CSID is a non-emergency resource for use by emergency responders across the nation. CSID is a comprehensive coordination, management, information, and scheduling tool developed by DHS through G&T for homeland security terrorism preparedness activities. The CSID provides general information on all DHS programs and information on the characteristics of CBRNE, agro-terrorism, defensive equipment, mitigation techniques, and available Federal assets and resources.

The CSID maintains a comprehensive database containing key personnel contact information for homeland security terrorism preparedness programs and events. These contacts include personnel at the Federal, State and local levels.

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

2. Office of Grant Operations (OGO). G&T's Office of Grant Operations will provide fiscal support, including pre- and post-award administration and technical assistance, of the grant programs included in this solicitation, with the exception of payment related issues.

For financial and administrative questions, all grant and sub-grant recipients should refer to the OGO *Financial Management Guide* or contact OGO at 1-866-9ASKOGO or *ask-ogo@dhs.gov*. All payment related questions should be referred to the Office of Justice Programs/Office of the Comptroller (OJP/OC) Customer Service at 1-800-458-0786 or *askoc@ojp.usdoj.gov*. All grant and sub-grant recipients should refer to the OGO *Financial Management Guide*.

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

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