



U.S. DEPARTMENT OF HOMELAND SECURITY

**Fiscal Year 2008**

**INFRASTRUCTURE PROTECTION PROGRAM:**

**BUFFER ZONE PROTECTION PROGRAM**

**GUIDANCE AND APPLICATION KIT**

**February 2008**



U.S. DEPARTMENT OF HOMELAND SECURITY

# CONTENTS

CONTENTS .....	I
INTRODUCTION.....	1
PART I. AVAILABLE FUNDING AND ELIGIBLE APPLICANTS .....	5
PART II. APPLICATION EVALUATION PROCESS .....	9
PART III. PROGRAM REQUIREMENTS.....	14
APPENDIX A. ALIGNMENT OF IPP WITH THE NATIONAL PREPAREDNESS ARCHITECTURE.....	A-1
APPENDIX B. BZPP ALLOWABLE EXPENSES .....	B-1
APPENDIX C. <i>GRANTS.GOV</i> QUICK-START INSTRUCTIONS .....	C-1
APPENDIX D. AWARD AND REPORTING REQUIREMENTS.....	D-1
APPENDIX E. ADDITIONAL RESOURCES .....	E-1

## INTRODUCTION

The Buffer Zone Protection Program (BZPP) is one of seven grant programs that constitute the Department of Homeland Security (DHS) Fiscal Year 2008 Infrastructure Protection Program (IPP).<sup>1</sup> The IPP is one tool among a comprehensive set of measures authorized by Congress and implemented by the Administration to help strengthen the nation's critical infrastructure against risks associated with potential terrorist attacks.

The vast bulk of America's critical infrastructure is owned and/or operated by State, local and private sector partners. The funds provided by the BZPP are provided to increase the preparedness capabilities of jurisdictions responsible for the safety and security of communities surrounding high-priority critical infrastructure and key resource (CIKR) 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 FEMA 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 CIKR. 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 Guidelines and its associated work products, including the National Infrastructure Protection Plan (NIPP) and the sector-specific plans (SSPs) located at <http://www.dhs.gov/nipp>. The National

---

<sup>1</sup> The IPP's other components include grants targeted for marine ports, transit (including Amtrak and freight rail security), intercity bus, and the trucking industry.

Preparedness Guidelines are an all-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 Guidelines define a vision of what to accomplish and a set of tools 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 Guidelines' success.<sup>2</sup> The Guidelines outline 15 scenarios of terrorist attacks or national disasters that form the basis of much of the Federal exercise and training regime. In addition, they identify some 37 critical capabilities that DHS is making the focus of key investments with State, local and tribal partners.

The NIPP Base Plan provides guidance to assist States in building and sustaining a statewide CIKR protection program. In accordance with the NIPP risk management framework and requirements identified in the FY 2007 HSGP, State governments must develop and implement a statewide/regional CIKR protection program as a component of their overarching homeland security program. This includes the necessary processes to implement the NIPP risk management framework at the State and/or regional level, including Urban Areas. More information can be found at <http://www.dhs.gov/nipp>

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 Guidelines 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 Fiscal Year (FY) 2008 BZPP, as a component of the IPP, provides funds to increase the preparedness capabilities of jurisdictions responsible for the safety and security of communities surrounding high-priority CIKR 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 CIKR assets. These capabilities are enumerated in Buffer Zone Plans (BZPs) that assist in:

- Identifying significant assets at the site(s) that may be targeted by terrorists for attack.
- Identifying specific threats and vulnerabilities associated with the site(s) and its

---

<sup>2</sup> The National Preparedness Guidelines and its supporting documents were published in September 2007. For purposes of aligning applications under the IPP, applicants can rely on the finalized Guidelines, available at: <http://www.fema.gov/pdf/government/npg.pdf>.

significant assets.

- Developing 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.
- Identifying 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 CIKR site(s) and appropriate points of contact within these organizations.
- Evaluating the capabilities of the responsible jurisdictions with respect to terrorism prevention and response.
- Identifying specific planning, equipment, training, and/or exercise requirements that 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.

FY 2008 BZPP funds should be coordinated with appropriate State POCs to support the development and implementation of a statewide/regional CIKR protection program, as described above. In addition, DHS is encouraging that State and local jurisdictions consider the following activities as priorities under the FY 2008 BZPP.

- 1. Coordination of Operational Activities with Public and Private Sector Partners.** DHS encourages that projects funded through the FY 2008 BZPP support coordination and direct interaction with private sector safety and security partners at the identified BZPP site. Examples include signing MOUs to allow facility security managers access to video camera surveillance feeds resulting from cameras purchased through the BZPP.
- 2. Coordination of Operational and Situational Awareness Activities with Fusion Centers and/or Emergency Operation Centers (EOCs).** DHS encourages projects funded through the FY 2008 BZPP to support coordination and direct interaction with State, regional, and/or Urban Area fusion centers, and/or EOCs located in the region of the identified BZPP site. Examples include allowing fusion centers and/or EOCs access to video camera surveillance feeds resulting from cameras purchased through the BZPP or ensuring the jurisdiction responsible for the BZPP site has an identified liaison officer responsible for coordinating with and reporting suspicious activity to the fusion center.
- 3. Multidisciplinary Involvement and Cooperation.** DHS encourages that projects funded through the FY 2008 BZPP support coordination and involvement of multidisciplinary partners in the development and implementation of preventive and protective measures, including emergency management and response, fire, public works, and public health personnel.

4. **Integration of the DHS CIKR Taxonomy in CIKR collection, storage/catalog, and reporting information technology (IT) solutions, databases, and processes.** DHS encourages those State and local jurisdictions leveraging IT solutions to support CIKR assessments and the development of BZPP documents, including the BZP and VRPP, to ensure these systems collect, store, categorize, and report CIKR information in accordance with the DHS CIKR Taxonomy, which is located at <https://odp.esportals.com/>.

### **C. Allowable Expenses**

Specific investments made in support of the funding priorities discussed above generally fall into three categories. FY 2008 BZPP allowable costs are therefore divided into the following three categories:

1. Planning
2. Equipment acquisitions
3. Management and administration (M&A)

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

## PART I. AVAILABLE FUNDING AND ELIGIBLE APPLICANTS

This section summarizes the total amount of funding available under the FY 2008 BZPP, the basic distribution method used to administer the grants, and the States that are eligible for FY 2008 funding.

### A. Available Funding

In FY 2008, the total amount of funds distributed under the BZPP will be \$48,575,000.

**A.1-- Potential for Future Cost Share Requirements.** Grantees are not required to provide a cash or in-kind cost share for FY 2008 BZPP funds. However, there is the potential for future grant programs to be impacted by cost share requirements as early as 2009. Accordingly, grantees should anticipate and plan for future homeland security programs to require cash or in-kind cost-share at levels comparable to other DHS administered grant programs.

### 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 CIKR 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. Several States have sites that are close in proximity. DHS will work closely with these States and provide supplemental guidance within the FY 2008 BZPP timelines to ensure coordinated planning<sup>3</sup>.

Through the FY 2008 BZPP, DHS continues to build on its cross-sector baseline knowledge of CIKR and the systematic approach initiated in FY 2006 to focus sufficient resources to reduce the risk associated with the highest priority CIKR assets across certain targeted sectors. These include:

---

<sup>3</sup> In the course of closing gaps at sites specifically identified by DHS in the 2008 BZPP, if a State has any residual grant funding remaining from the allocation provided upon completion of all necessary activities to develop and implement a BZP at the DHS selected site(s), the State may redirect the residual funds to another CIKR site, subject to justification and DHS final approval.

- Highest consequence chemical facilities
- Nuclear power plants
- Higher consequence liquified natural gas facilities
- Critical water/wastewater systems
- Higher consequence dams
- Transportation system critical nodes
- Critical telecommunications facilities
- Critical banking and finance facilities
- Critical public health and healthcare facilities
- Select food and agriculture facilities

### **B.1 -- Characterization of CIKR Tiers.**

DHS has established a set of consequence thresholds to identify sites that are considered CIKR *Tier 1* assets, and thus eligible for higher funding levels. To be considered CIKR *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.<sup>4</sup> 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 CIKR *Tier 2* assets that would identify those CIKR 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. CIKR sites that may otherwise meet the criteria identified above, but are not being addressed through the FY 2008 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 analysis builds upon the program plan and methodology in place last year. *Tier 1* and *Tier 2* assets have been prioritized, and funds are being systematically applied to address the list of assets supported by the BZPP. Based upon the results of

---

<sup>4</sup> 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.

DHS 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 FY 2008 BZPP.<sup>5</sup> The specific sites and their locations are sensitive and DHS has directly contacted each State with information regarding the identity and location, as well as funding amounts of the selected high-risk sites in their area.

**Table 1. FY 2008 BZPP Funding Allocations**

<b>State/Territory</b>	<b>Allocation</b>	<b>State/Territory</b>	<b>Allocation</b>
Alabama	\$796,000	Montana	\$199,000
Alaska	\$398,000	Nebraska	\$995,000
Arizona	\$597,000	Nevada	\$398,000
California	\$7,379,000	New Jersey	\$995,000
Colorado	\$1,597,000	New Mexico	\$597,000
Connecticut	\$398,000	New York	\$4,485,000
District of Columbia	\$1,172,000	North Carolina	\$597,000
Florida	\$1,791,000	Ohio	\$1,194,000
Georgia	\$1,592,000	Oklahoma	\$199,000
Guam	\$398,000	Oregon	\$995,000
Hawaii	\$398,000	Pennsylvania	\$796,000
Illinois	\$2,189,000	Rhode Island	\$199,000
Indiana	\$398,000	South Carolina	\$398,000
Iowa	\$1,194,000	Tennessee	\$199,000
Kansas	\$597,000	Texas	\$4,184,000
Kentucky	\$597,000	Utah	\$398,000
Louisiana	\$3,092,000	Virginia	\$199,000
Maryland	\$1,791,000	Washington	\$796,000
Massachusetts	\$398,000	West Virginia	\$597,000
Michigan	\$995,000	Wisconsin	\$199,000
Minnesota	\$597,000	Wyoming	\$597,000
Mississippi	\$199,000	Commonwealth of Puerto Rico	\$199,000
Missouri	\$597,000		
<b>Total</b>			<b>\$48,575,000</b>

<sup>5</sup> Jurisdictions responsible for select FY 2008 BZPP sites identified for funding, which include cable landing stations, will be required to leverage FY 2008 BZPP funds to support the implementation of preventive and protective measures associated with manhole covers located in close proximity to the site. These specific site details are sensitive and OIP will directly contact affected States with information regarding the site(s), as well as the implementation of any required preventive and/or protective measures associated with the site(s).

### 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.<sup>6</sup> 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.<sup>7</sup> The SAA must coordinate all BZPP activities with the respective State Homeland Security Advisor (HSA). Each State shall make no less than **97 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 CIKR assets. It 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.

---

<sup>6</sup> 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.”

<sup>7</sup> As defined in the Conference Report accompanying the Department of Homeland Security Appropriations Act of 2008, 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 FY 2008 BZPP program, and core process and priorities that will be used to assess applications under the FY 2008 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 FEMA via [grants.gov](http://grants.gov) (see below for details about this Federal grants application tool) *no later than 11:59 PM EDT, March 17, 2008.*

Applicants must comply with all administrative requirements -- including budgets and application process requirements -- described herein.

### B. BZPP Coordination Requirements

Use of FY 2008 BZPP funds must be consistent with the State and/or Urban Area Homeland Security Strategy. Therefore, the BZP and VRPP must be coordinated between the SAA and State Homeland Security Advisor (HSA), as well as any applicable State strategy planning teams, Urban Area Working Groups (UAWGs), Regional Transit Security Working Groups (RTSWGs), and/or Area Maritime Security Committees (AMSCs), as applicable.

**B.1 -- State Coordination.** Upon completion of the BZP and VRPP, the responsible jurisdiction must submit the BZP and VRPP to the SAA (in coordination with the HSA) for:

- Coordination of the BZPP with State Homeland Security Strategies, priorities, and programs;
- Coordination with related HSGP and IPP funding; and,
- Certification that the BZP and VRPP supports and/or compliments: a) Statewide efforts to develop a CIKR protection program and implement CIKR protection capabilities, as directed in the NIPP, and b) the implementation of the NIPP as a national priority, as reflected within each respective State's homeland security strategy.

**B.2 -- Private Sector Coordination.** CIKR assets are 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.3 -- Urban Area Working Group (UAWG) 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 the development and implementation of all UASI program initiatives, Urban Area Homeland Security Strategy development, and any direct services that are delivered by DHS. 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.

**B.4 – Protective Security Advisor (PSA) Coordination.** DHS has deployed PSAs in major metropolitan areas throughout the country to assist State and local efforts to identify and protect CIKR and to ensure national risk assessments are better informed through State and local input. PSAs implement DHS's mission to protect CIKR by fostering improved coordination at the State and local level through their support for national CIKR protection-related programs. Responsible jurisdictions must coordinate with and include their PSAs in the assessment of CIKR identified for BZPP funding to ensure all necessary resources are made available for the development of the BZP.

### **C. Buffer Zone Plans (BZPs) and Vulnerability Reduction Purchasing Plans (VRPPs)**

**C.1 -- Development of the BZP and VRPP.** The IP Protective Security Coordination Division (PSCD) provides a range of support to BZPP grantees and sub-grantees. PSCD can provide a federally guided vulnerability assessment team to assist in the development of the BZP. BZP workshops, which train law enforcement and other homeland security prevention personnel on the BZP process, are also available to support grantee and sub-grantee jurisdictions.

While conducting a BZP assessment with DHS assistance, a Site Assistance Visit (SAV) will also be conducted, when possible. The purpose of conducting a SAV in coordination with the BZP assessment is to provide the CIKR owner and operator with a facility report. This coordinated process reduces the need to revisit a site for a more detailed assessment, thus reducing the impact on owner/operators and on State and local homeland security personnel. Additionally, conducting these assessments simultaneously will provide a more thorough BZP and SAV report for State, local, and private sector partners to support prevention and protection efforts of CIKR.

- Jurisdictions are required to notify and include their PSAs in the BZP assessment. The PSA will coordinate federal resources to ensure the appropriate level of support and/or resources are available during the BZP workshop and/or assessment.
- 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 CIKR 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 DHS, upon request, 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 responsible jurisdictions must complete the BZP template in coordination with the State for each identified CIKR site. Additionally, the development of the BZP must be coordinated with the following entities, as applicable and when possible:
  - Urban Area Working Groups (UAWGs)
  - Area Maritime Security Committees (AMSCs)
  - Regional Transit Security Working Groups (RTSWGs)
  - Protective Security Advisors (PSAs)
  - Sector Specific Agencies (SSAs) (information on the SSAs located at [http://www.dhs.gov/xlibrary/assets/NIPP\\_SectorOverview.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_SectorOverview.pdf))

The BZP template serves as a useful tool that can be integrated to support CIKR protection program planning efforts across all sectors. The BZP will assist in identifying preventive and protective measures necessary to protect the CIKR site, mitigate vulnerabilities, or close capability gaps. This includes a description of required planning, equipment, training, and exercises 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. If multiple sites are identified in a single VRPP, the responsible jurisdictions should ensure that any requested equipment is available to support the implementation of preventive and protective measures for all identified sites in the VRPP, as appropriate and applicable. For more information on assessments or the assessment process, please contact [ipassessment@dhs.gov](mailto:ipassessment@dhs.gov).

## **C.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 CIKR 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, implement, and/or operate a CIKR 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.
  - These certifications and concurrences must be comprehensively detailed by the SAA within the SAA section of the VRPP.
  - If requesting PCII protection, the SAA must complete the Express and Certification Statements located within the BZP. The templates must remain in their original format if PCII protection is requested (i.e., Excel and Word). If PCII protection is not requested, the Express and Certification statements should be removed from the BZP template prior to submission.
- Upon certification, the SAA must submit the BZP and VRPP for each site to DHS for approval by **November 30, 2008**. ***If States fail to submit all BZPP materials by this date, funds may be deobligated by DHS.***
- The BZPs and VRPPs must be submitted electronically via *the FEMA Secure Portal* located at: <https://odp.esportals.com/>. The *Secure Portal* will contain a FY 2008 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 allowable and coordinated with overall Statewide CIKR 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](mailto:BZPP@dhs.gov) email address. The actual BZPs and VRPPs themselves should never be sent via email.

- Funds under the FY 2008 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.

## PART III. PROGRAM REQUIREMENTS

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

### A. General Program Requirements

The applicable SAAs will be responsible for administration of the FY 2008 BZPP.

**Grant funds.** States must pass-through at a minimum, 97 percent of BZPP grant funds. Any funds retained by the State on behalf of BZPP for management and administrative purposes must be used in direct support of the BZPP jurisdiction.

DHS will track the congressionally-mandated obligation of funds to local units of government through each State's Initial Strategy Implementation Plan. In addition, DHS strongly encourages the timely obligation of funds from local units of government to other subgrantees, as appropriate.

**Management and Administration (M&A) limits.** A maximum of three percent (3%) of funds awarded may be retained by the State, and any funds retained are to be used solely for management and administrative purposes associated with the BZPP award. States may pass through a portion of the State M&A allocation to local subgrantees to support local management and administration activities.

### B. Application Requirements

The following steps must be completed using the on-line [grants.gov](http://www.grants.gov) system to ensure a successful application submission, however applicants should review the relevant program-specific sections of this Guidance for additional requirements that may apply.

1. **Application via [grants.gov](http://www.grants.gov).** DHS participates in the Administration's e-government initiative. As part of that initiative, all applicants must file their applications using the Administration's common electronic "storefront" -- [grants.gov](http://www.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](http://www.grants.gov) no later than **11:59 PM EST, March 17, 2008**.
3. **Valid Central Contractor Registry (CCR) Registration.** The application process also involves an updated and current registration by the applicant. Eligible

applicants must confirm CCR registration at <http://www.ccr.gov>, as well as apply for funding through [grants.gov](http://grants.gov).

4. **On-line application.** The on-line application must be completed and submitted using [grants.gov](http://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 “*The 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. Extensions to the period of performance will be considered on a case-by-case basis only through formal written requests to DHS.
6. **DUNS number.** The applicant must provide a Dun and Bradstreet Data Universal Numbering System (DUNS) number with their application. This number is a required field within [grants.gov](http://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. **State Preparedness Report.** PKEMRA requires any State that receives Federal preparedness assistance to submit a State Preparedness Report to DHS. For FY 2008, the State Preparedness Report consolidates existing requirements into a single submission, including updates to the Nationwide Plans Review (NPR) Phase 1; development of the Program Evaluation Report, as required in FY 2007 HSGP; and updates to the State Program and Capability Enhancement Plan.

State Preparedness Reports must be submitted to DHS by March 31, 2008.

**Receipt is a prerequisite for applicants to receive any FY 2008 DHS preparedness grant funding.**

State Preparedness Reports will be marked and handled as “For Official Use Only” due to the sensitive nature of the information contained in them. DHS has established a secure internet portal at <https://odp.esportals.com/> to receive and manage all State Preparedness Reports in order to safeguard them and any information identifying potential shortcomings.

**8. Single Point of Contact (SPOC) review.** Executive Order 12372 requires applicants from State and local units of government or other organizations providing services within a State to submit a copy of the application to the State SPOC, if one exists, and if this program has been selected for review by the State. Applicants must contact their State SPOC to determine if the program has been selected for State review. Executive Order 12372 can be referenced at <http://www.archives.gov/federal-register/codification/executive-order/12372.html>.

**9. Standard financial requirements.**

**9.1 -- 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. 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.

**9.2 -- Assurances.** Assurances forms (SF-424B and SF-424D) can be accessed at [http://www07.grants.gov/agencies/approved\\_standard\\_forms.jsp](http://www07.grants.gov/agencies/approved_standard_forms.jsp). It is the responsibility of the recipient of the Federal funds to understand fully 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.

**9.3 -- Certifications regarding lobbying, debarment, suspension, other responsibility matters and the 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 44 CFR Part 17, which contains provisions for *Government-wide Debarment and Suspension (Non-procurement)* and *Government-wide Requirements for Drug-Free Workplace (Grants)*; and 44 CFR part 18, *the New Restrictions on Lobbying*. All of these can be referenced at: [http://www.access.gpo.gov/nara/cfr/waisidx\\_07/44cfrv1\\_07.html](http://www.access.gpo.gov/nara/cfr/waisidx_07/44cfrv1_07.html)  
[http://www.access.gpo.gov/nara/cfr/waisidx\\_00/44cfrv1\\_00.html](http://www.access.gpo.gov/nara/cfr/waisidx_00/44cfrv1_00.html).

**10. Technology requirements.**

**10.1 -- National Information Exchange Model (NIEM).** DHS requires all grantees to use the latest NIEM specifications and guidelines regarding the use of Extensible Markup Language (XML) for all BZPP awards. Further information about the required use of NIEM specifications and guidelines is available at <http://www.niem.gov>.

**10.2 -- 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). DHS encourages grantees to align any

geospatial activities with the guidance available on the FEMA website at <http://www.fema.gov/government/grant/index.shtm>.

**10.3 -- 28 CFR Part 23 guidance.** DHS requires that any information technology system funded or supported by BZPP funds comply with 28 CFR Part 23, Criminal Intelligence Systems Operating Policies, if this regulation is determined to be applicable.

## **11. Administrative requirements.**

**11.1 -- 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. 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 FEMA regarding concerns or questions about the release of information under State and local laws. The grantee should be familiar with the regulations governing Sensitive Security Information (49 CFR Part 1520), as it may provide additional protection to certain classes of homeland security information.

**11.2 -- 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](mailto:pcii-info@dhs.gov).

**11.3 -- 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 funds 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. .
- *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. .
- *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.
- *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.

**11.4 -- 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, natural 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 Investment Justifications 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>.

**11.5 -- Integrating individuals with disabilities into emergency planning.** Section 504 of the Rehabilitation Act of 1973, as amended, prohibits discrimination

against people with disabilities in all aspects of emergency mitigation, planning, response, and recovery by entities receiving financial from DHS. In addition, Executive Order #13347, entitled "Individuals with Disabilities in Emergency Preparedness" 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. Executive Order 13347 requires the federal government to, among other things, encourage consideration of the needs of individuals with disabilities served by State, local, and tribal governments in emergency preparedness planning.

DHS has several resources available to assist emergency managers in planning and response efforts related to people with disabilities and to ensure compliance with Federal civil rights laws:

- **Guidelines for Accommodating Individuals with Disabilities in Disaster:** The Guidelines synthesize the array of existing accessibility requirements into a user friendly tool for use by response and recovery personnel in the field. The Guidelines are available at <http://www.fema.gov/oe/reference/>.
- **Disability and Emergency Preparedness Resource Center:** A web-based "Resource Center" that includes dozens of technical assistance materials to assist emergency managers in planning and response efforts related to people with disabilities. The "Resource Center" is available at <http://www.disabilitypreparedness.gov>.
- *Lessons Learned Information Sharing (LLIS)* resource page on **Emergency Planning for Persons with Disabilities and Special Needs:** A true one-stop resource shop for planners at all levels of government, non-governmental organizations, and private sector entities, the resource page provides more than 250 documents, including lessons learned, plans, procedures, policies, and guidance, on how to include citizens with disabilities and other special needs in all phases of the emergency management cycle.

LLIS.gov is available to emergency response providers and homeland security officials from the local, state, and federal levels. To access the resource page, log onto <http://www.LLIS.gov> and click on *Emergency Planning for Persons with Disabilities and Special Needs* under *Featured Topics*. If you meet the eligibility requirements for accessing Lessons Learned Information Sharing, you can request membership by registering online.

**11.6 -- Compliance with the National Energy Conservation Policy and Energy Policy Acts.** In accordance with the Consolidated Appropriations Act of 2008 (P.L. 110-161), all FY 2008 grant funds must comply with the following two requirements:

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

**11.7 -- Environmental and Historic Preservation Compliance.** FEMA is required to consider the potential impacts to the human and natural environment of projects proposed for FEMA funding. FEMA, through its Environmental and Historic Preservation (EHP) Program, engages in a review process to ensure that FEMA-funded activities comply with various Federal laws including: National Environmental Policy Act, National Historic Preservation Act, Endangered Species Act, and Executive Orders on Floodplains (11988), Wetlands (11990) and Environmental Justice (12898). The goal of these compliance requirements is to protect our nation's water, air, coastal, wildlife, agricultural, historical, and cultural resources, as well as to minimize potential adverse effects to children and low-income and minority populations.

The grantee shall provide any information requested by FEMA to ensure compliance with applicable Federal EHP requirements. Any project with the potential to impact EHP resources (see Section E.8) cannot be initiated until FEMA has completed its review. Grantees may be required to provide detailed information about the project, including the following: location (street address or map coordinates); description of the project including any associated ground disturbance work, extent of modification of existing structures, construction equipment to be used, staging areas, access roads, etc; year the existing facility was built; natural, biological, and/or cultural resources present in the project vicinity; visual documentation such as site and facility photographs, project plans, maps, etc; and possible project alternatives.

For certain types of projects, FEMA must consult with other Federal and state agencies such as the U.S. Fish and Wildlife Service, State Historic Preservation Offices, and the U.S. Army Corps of Engineers, as well as other agencies and organizations responsible for protecting natural and cultural resources. For projects with the potential to have significant adverse effects on the environment and/or historic properties, FEMA's EHP review and consultation may result in a substantive agreement between the involved parties outlining how the grantee will avoid the effects, minimize the effects, or, if necessary, compensate for the effects.

Because of the potential for significant adverse effects to EHP resources or public controversy, some projects may require an additional assessment or report, such as an Environmental Assessment, Biological Assessment, archaeological survey, cultural resources report, wetlands delineation, or other document, as well as a public comment period. Grantees are responsible for the preparation of such

documents, as well as for the implementation of any treatment or mitigation measures identified during the EHP review that are necessary to address potential adverse impacts. Grantees may use BZPP funds toward the costs of preparing such documents and/or implementing treatment or mitigation measures. Failure of the grantee to meet Federal, State, and local EHP requirements, obtain applicable permits, and comply with any conditions that may be placed on the project as the result of FEMA's EHP review may jeopardize Federal funding.

For more information on FEMA's EHP requirements, SAAs should refer to FEMA's Information Bulletin #271, *Environmental Planning and Historic Preservation Requirements for Grants*.

## APPENDIX A. ALIGNMENT OF IPP WITH THE NATIONAL PREPAREDNESS ARCHITECTURE

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

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



## **APPENDIX B.**

# **BZPP ALLOWABLE EXPENSES**

### **A. Overview**

FY 2008 BZPP allowable costs are divided into the following three categories:

1. Planning
2. Equipment acquisitions
3. Management and administration (M&A)

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 FY 2008 BZPP. Grantees are encouraged to contact their Preparedness Officer regarding authorized and unauthorized expenditures.

**1. Planning.** Planning activities are central to the implementation of the BZPP. The BZPP is designed as a planning tool to integrate the efforts of local agencies and their private sector partners. Accordingly, responsible jurisdictions may use BZPP programmatic funds to support multi-discipline prevention and protection-focused planning activities specific to the selected facility. However the priority should continue to be on mitigating equipment and resource shortfalls identified in the development of the BZPP. Grantees should also confer with their local and State homeland security partners to determine additional funding source opportunities for planning-related purposes (such as FEMA's Homeland Security Grant Programs). Examples of allowable planning costs for the individual BZPP activities can be found at <http://www.fema.gov/grants>.

FY 2008 BZPP funds may be used for a range of homeland security and CIKR protection planning activities, such as:

#### **1.1 -- Developing and implementing homeland security and CIKR support programs and adopting DHS national initiatives limited to the following:**

- Implementing the National Preparedness Guidelines, as it relates to implementation of the NIPP, and SSPs.
- Building or enhancing preventive radiological and nuclear detection programs.
- Modifying existing incident management and Emergency Operating Plans (EOPs) to ensure proper alignment with the National Response Framework (NRF) and the NIMS coordinating structures, processes, and protocols.

- Establishing or enhancing mutual aid agreements or MOUs to ensure cooperation with respect to CIKR protection.
- Developing communications and interoperability protocols and solutions with the BZPP 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 (NIC).
- 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 CIKR 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 CIKR 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.us>. DHS-adopted standards can be found at [http://www.dhs.gov/xfrstresp/standards/editorial\\_0420.shtm](http://www.dhs.gov/xfrstresp/standards/editorial_0420.shtm).

The Responder Knowledge Base houses the AEL and the Standardized Equipment List (SEL). In some cases, items on the SEL are not allowable under FY 2008 BZPP, or will not be eligible for purchase unless specific conditions are met. Unless otherwise specified, maintenance costs/contracts for authorized equipment purchased using FY 2008 BZPP funding or acquired through the DHS Homeland Defense Equipment Reuse (HDER) 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
[14]	Physical Security Enhancement Equipment
[15]	Inspection and Screening Systems
[16]	Agricultural Terrorism Prevention, Response, and Mitigation Equipment
[20FP]	Intervention Equipment - Equipment, Fingerprint Processing, and Identification*

\* Only select sub-categories within AEL Category 3 and 20 are eligible for FY 2008 BZPP funding. These sections include: 3OE-02, 3OE-07, 03SR-03-LSTN, 03OE-03-LTPA, 03OE-04-LTHH, 03OE-04-LTHE, 03SR-03-SCAM, 03SR-05, 03WA-01-PROP, 03WA-01-ULHH, 03WA-01-ULIT, 03WA-01-UWMD, 03WA-02-SONR, and 20FP.

Other specialized equipment not listed in the BZPP 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 all of the following to their FEMA Preparedness Officer, who, in consultation with IP, will review the request.

- 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 FY 2008 BZPP site and its

responsible jurisdiction, as identified by the BZP (i.e., PPE for a jurisdiction responsible for a chemical facility or watercraft for a dam).

- 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.** A maximum of up to three percent (3%) of funds awarded may be retained by the State, and any funds retained are to be used solely for management and administrative purposes associated with the BZPP award. States may pass through a portion of the State M&A allocation to local subgrantees to support local management and administration activities.

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 FY 2008 BZPP.
  - To assist with the coordination and implementation requirements of the FY 2008 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.
  - FY 2008 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 FY 2008 BZPP.

## **B. Unallowable Costs.**

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

- **Hiring of Public Safety Personnel.** FY 2008 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 FY 2008 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. However, if an identified FY 2008 BZPP site is a federal facility, the FY 2008 BZPP funds may be used by the jurisdiction(s), responsible for the safety and security of the community surrounding the site, to support the implementation of preventive and protective measures in the buffer zone surrounding that site.
- **Overtime and Backfill.** Funds may not be used to support overtime and backfill costs associated with implementation of FY 2008 BZPP activities.
- **Training and Exercise Activities.** Any resulting training or exercise requirements identified through the BZPP may not be funded with FY 2008 BZPP funds, but may be funded through other overarching homeland security grant programs (i.e. State Homeland Security Program (SHSP), and Urban Areas Security Initiative (UASI)) in accordance with their stipulated authorized expenditures.

Additionally, the following initiatives and costs are considered **ineligible** for award consideration:

- Initiatives that do not address the implementation of programs/initiatives to build prevention and protection-focused 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 C. GRANTS.GOV QUICK-START INSTRUCTIONS

DHS participates in the Administration’s e-government initiative. As part of that initiative, all IPP applicants must file their applications using the Administration’s common electronic “storefront” -- [grants.gov](http://www.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](http://www.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](http://www.grants.gov).

This Appendix is intended to provide guidance on the various steps and activities associated with filing an application using [grants.gov](http://www.grants.gov).

### Step 1: Registering.

Registering with [grants.gov](http://www.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](http://www.grants.gov) requires an organization to first be registered in the CCR before beginning the [grants.gov](http://www.grants.gov) registration process. If you plan to authorize representatives of your organization to submit grant applications through [grants.gov](http://www.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](http://www.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](http://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 (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](http://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 (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://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/AORRegCheck.pdf](http://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 (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](http://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](http://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](https://www.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](https://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](https://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](http://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](http://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](http://grants.gov). The confirmation e-mail will give you a [grants.gov](http://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](http://grants.gov). To do this, go to the [grants.gov](http://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](https://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](https://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](https://grants.gov) or GMS due to errors. You will receive an e-mail from [grants.gov](https://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](https://grants.gov) customer support hotline at (800) 518–4726.

## **APPENDIX D.**

# **AWARD AND REPORTING REQUIREMENTS**

Prior to the transition to FEMA, the former Office of Grants and Training preparedness programs followed The Department of Justice's codified regulations, 28 CFR and the OGO Financial Management Guide. The former Office of Grants and Training is now within FEMA and all preparedness programs will follow FEMA's codified regulations, 44 CFR.

### **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.”

Obligations are a legal liability to pay, under a grant, subgrant, or contract, determinable sums for services or goods incurred during the grant period. This includes, but is not limited to, amounts of orders placed, contracts and subgrants awarded, goods and services received, and similar transactions during a given period that will require payment by the grantee during the same or a future period.

Awards made to SAAs under this program carry additional pass-through requirements. Pass-through is defined as an obligation on the part of the States to make funds available to units of local governments, combinations of local units, or other specific groups or organizations. The State’s pass-through period must be met within 45 days of the award date for BZPP. Four requirements must be met to pass-through grant funds:

- There must be some action to establish a firm commitment on the part of the awarding entity.
- The action must be unconditional (i.e., no contingencies for availability of SAA funds) on the part of the awarding entity.
- There must be documentary evidence of the commitment.
- The award terms must be communicated to the official grantee.

The period of performance is 36 months. Any unobligated funds will be deobligated at the end of this period. Extensions to the period of performance will be considered only through formal requests to FEMA with specific and compelling justifications why an extension is required.

## B. Post Award Instructions

The following is provided as a guide for the administration of an award. 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 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. Follow the directions in the notification e-mail and log into GMS to access the award documents. The authorized grantee official should carefully read the award and special condition documents. If you do not receive a notification e-mail, please contact your Preparedness Officer for your award number. Once you have the award number, contact the GMS Help Desk at (888) 549-9901, option 3 to obtain the username and password associated with the new award.

If you agree with the terms and conditions, the authorized grantee official should sign and date both the original and the copy of the award document page in Block 19 and initial the special conditions page(s). Retain a copy and fax the documents to (202) 786-9905 Attention: Control Desk or send the original signed documents to:

**U.S. Department of Homeland Security/FEMA  
Grant Programs Directorate/Control Desk 4<sup>th</sup> Floor, TechWorld  
500 C St SW  
Washington, DC 20472**

If you do not agree with the terms and conditions, contact the Preparedness Officer named in the award package.

**2. Complete and return form SF1199A .** The SF1199A Direct Deposit Sign-up Form is used to set up direct deposit for grant payments. The SF1199A form can be found at: <http://www.fema.gov/grants>.

NOTE: Please include your vendor number in Box C of the SF1199A form.

**3 Access to payment systems.** Grantees under this solicitation will use FEMA's online Payment and Reporting System (PARS) to request funds. The website to access PARS is <https://isource.fema.gov/sf269/execute/Login?sawContentMessage=true>. Questions regarding payments or how to access PARS should be directed to the FEMA Call Center at (866) 927-5646 or sent via e-mail to [ask-OGO@dhs.gov](mailto:ask-OGO@dhs.gov).

**4. Reporting requirements.** Reporting requirements must be met throughout the life of the grant (refer to the program guidance and the special conditions found in the award package for a full explanation of these requirements. Please note that PARS contains edits that will prevent access to funds if reporting requirements are not met on a timely basis.

**5. Questions about your award?** A reference sheet is provided containing frequently asked financial questions and answers. Financial management questions regarding your award should be directed to the FEMA Call Center at (866) 927-5646 or sent via e-mail to [ask-OGO@dhs.gov](mailto: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, please contact the GMS Help Desk at (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 PARS.

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. FEMA 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 44 CFR Part 13, Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments and 2 CFR Part 215, Uniform Administrative Requirements for Grants and Agreements (Including Sub-awards) with Institutions of Higher Education, Hospitals and other Non-profit Organizations (formerly OMB Circular A-110). These regulations further provide 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 grantee may keep interest earned, up to \$100 per fiscal year for administrative expenses. This maximum limit is not per award; it is inclusive of all interest earned on all Federal grant program funds received.

Although advance drawdown requests are permissible, 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 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 no later than April 30). A report must be submitted for every quarter of the period of performance, including partial calendar quarters, as well as for periods where no grant activity occurs. Future awards and fund draw downs may be withheld if these reports are delinquent. The final FSR is due 90 days after the end date of the performance period.

FSRs **must be filed online** through the PARS.

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

**2. Biannual Strategy Implementation Reports (BSIR) and Categorical Assistance Progress Report (CAPR).** Following an award, the grantee will be responsible for providing updated obligation and expenditure information on a semi-annual basis. The applicable SAAs are responsible for completing and submitting the CAPR/BSIR reports. The BSIR submission will satisfy the narrative requirement of the CAPR. SAAs are still required to submit a CAPR with a statement in the narrative field that states: “See BSIR.”

The BSIR and the CAPR are due within 30 days after the end of the reporting period (July 30 for the reporting period of January 1 through June 30; and January 30 for the reporting period of July 1 through December 31). Updated obligations and expenditure information must be provided with the BSIR to show progress made toward meeting strategic goals and objectives. Future awards and fund drawdowns may be withheld if these reports are delinquent.

CAPRs must be filed online through the internet at <http://grants.ojp.usdoj.gov>. Guidance and instructions for completing the CAPR can be found at <https://grants.ojp.usdoj.gov/gmsHelp/index.html>.

***Required submission: BSIR and CAPR (due semi-annually).***

**3. Exercise Evaluation and Improvement.** Exercises implemented with grant funds should be threat- and performance- based and should evaluate performance of critical prevention and response tasks required to respond to the exercise scenario. Guidance on conducting exercise evaluations and implementing improvement is defined in the *Homeland Security Exercise and Evaluation Program (HSEEP) Volume II: Exercise Evaluation and Improvement* located at <http://www.hseep.dhs.gov>. Grant recipients must report on scheduled exercises and ensure that an After Action Report (AAR) and

Improvement Plan (IP) are prepared for each exercise conducted with FEMA support (grant funds or direct support) and submitted to FEMA within 60 days following completion of the exercise.

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

***Required submissions: AARs and IPs (as applicable).***

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

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

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

**6. National Preparedness Reporting Compliance.** The Government Performance and Results Act (GPRA) requires that the Department collect and report performance information on all programs. For grant programs, the prioritized Investment Justifications and their associated milestones provide an important tool for assessing

grant performance and complying with these national preparedness reporting requirements. FEMA 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.

#### **E. Monitoring.**

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

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

#### **F. Grant Close-Out Process.**

Within 90 days after the end of the award period, SAAs must submit a final FSR and final CAPR detailing all accomplishments throughout the project. After these reports have been reviewed and approved by FEMA, 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 GPD, the grant will be identified as “Closed by the Grant Programs Directorate.”

***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 E. 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 FEMA for homeland security terrorism preparedness activities. The CSID provides general information on all FEMA preparedness grant 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 (800) 368-6498 or [askcsid@dhs.gov](mailto:askcsid@dhs.gov). CSID hours of operation are from 8:00 am–6:00 pm (EST), Monday-Friday.

**2. Grant Programs Directorate (GPD).** FEMA GPD will provide fiscal support, including pre- and post-award administration and technical assistance, to the grant programs included in this solicitation.

For financial and administrative guidance, all state and local government grant recipients should refer to 44 CFR Part 13, Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments. Institutions of higher education, hospitals, and other non-profit organizations should refer to 2 CFR Part 215 for the applicable uniform administrative requirements.

Additional guidance and information can be obtained by contacting the FEMA Call Center at (866) 927-5646 or via e-mail to [ask-OGO@dhs.gov](mailto:ask-OGO@dhs.gov).

**3. GSA's Cooperative Purchasing Program.** The U.S. General Services Administration (GSA) offers two efficient and effective procurement programs for State and local governments to purchase products and services to fulfill homeland security and other technology needs. The GSA Schedules (also referred to as the Multiple Award Schedules and the Federal Supply Schedules) are long-term, indefinite delivery, indefinite quantity, government-wide contracts with commercial firms of all sizes.

- Cooperative Purchasing Program  
Section 211 of the E-Government Act of 2002, authorized GSA sales of Schedule 70 IT products and services to State and Local Governments through the introduction of Cooperative Purchasing. The Cooperative Purchasing program

allows State and local governments to purchase from Schedule 70 (the Information Technology Schedule) and the Consolidated Schedule (containing IT Special Item Numbers) **only**. Cooperative Purchasing is authorized by Federal law and was enacted when Section 211 of the E-Government Act of 2002 amended the Federal Property and Administrative Services Act.

Under this program, State and local governments have access to over 3,500 GSA Schedule contractors who have voluntarily modified their contracts to participate in the Cooperative Purchasing program. The U.S. General Services Administration provides a definition of State and local governments as well as other vital information under the frequently asked questions section on its website at <http://www.gsa.gov/cooperativepurchasing>.

- **Disaster Recovery Purchasing Program**  
GSA plays a critical role in providing disaster recovery products and services to Federal agencies. Now State and Local Governments can also benefit from the speed and savings of the GSA Federal Supply Schedules. Section 833 of the John Warner National Defense Authorization Act for Fiscal Year 2007 (Public Law 109-364) amends 40 U.S.C. 502 to authorize the GSA to provide State and Local governments the use of ALL Federal Supply Schedules of the GSA for purchase of products and services to be used to *facilitate recovery from a major disaster declared by the President under the Robert T. Stafford Disaster Relief and Emergency Assistance Act or to facilitate **recovery** from terrorism or nuclear, biological, chemical, or radiological attack.*

In the aftermath of emergency events, State or local governments' systems may be disrupted. Thus, use of Federal Supply schedule contracts prior to these events to acquire products or services to be used to facilitate recovery is authorized. State or local governments will be responsible for ensuring that purchased products or services are to be used to facilitate recovery.

GSA provides additional information on the Disaster Recovery Purchasing Program website at <http://www.gsa.gov/disasterrecovery>.

State and local governments can find a list of eligible contractors on GSA's website, <http://www.gsa.library.gsa.gov>, denoted with a  or  symbol.

Assistance is available from GSA on the Cooperative Purchasing and Disaster Purchasing Program at the local and national levels. For assistance at the local level, visit <http://www.gsa.gov> to find the point of contact in your area. For assistance at the national level, contact Tricia Reed at [patricia.reed@gsa.gov](mailto:patricia.reed@gsa.gov), 571-259-9921. More information is available at <http://www.gsa.gov/cooperativepurchasing> and <http://www.gsa.gov/disasterrecovery>.

**4. Exercise Direct Support.** DHS has engaged multiple contractors with significant experience in designing, conducting, and evaluating exercises to provide support to States and local jurisdictions in accordance with State Homeland Security Strategies

and HSEEP. Contract support is available to help States conduct an Exercise Plan Workshop, develop a Multi-year Exercise Plan and build or enhance the capacity of States and local jurisdictions to design, develop, conduct, and evaluate effective exercises.

In FY 2008, States may receive direct support for three exercises: one Training & Exercise Plan Workshop (T&EPW); one discussion-based exercise; and one operations-based exercise. While States are allowed to submit as many direct support applications as they choose, they are strongly encouraged to give careful thought to which exercises will require the additional assistance that will be provided through the direct support program. Exercises involving cross-border or mass-gathering issues will be counted against the number of direct-support exercises being provided to States.

Applications for direct support are available at <http://hseep.dhs.gov> and are reviewed on a monthly basis. The Homeland Security Exercise and Evaluation Program offers several tools and resources to help design, develop, conduct and evaluate exercises.

**5. Homeland Security Preparedness Technical Assistance Program.** The Homeland Security Preparedness Technical Assistance Program (HSPTAP) provides technical assistance on a first-come, first-served basis (and subject to the availability of funding) to eligible organizations to enhance their capacity and preparedness to respond to CBRNE terrorist incidents. In addition to the risk assessment assistance already being provided, FEMA also offers a variety of other technical assistance programs.

More information can be found at <http://www.fema.gov/grants>.

**6. Lessons Learned Information Sharing (LLIS) System.** LLIS is a national, online, secure website that houses a collection of peer-validated lessons learned, best practices, AARs from exercises and actual incidents, and other relevant homeland security documents. LLIS facilitates improved preparedness nationwide by providing response professionals with access to a wealth of validated front-line expertise on effective planning, training, equipping, and operational practices for homeland security.

The LLIS website also includes a national directory of responders and homeland security officials, as well as an updated list of homeland security exercises, events, and conferences. Additionally, LLIS includes online collaboration tools, including secure e-mail and message boards, where users can exchange information. LLIS uses strong encryption and active site monitoring to protect all information housed on the system. The LLIS website is <https://www.llis.gov>.

**7. Information Sharing Systems.** DHS encourages all State, regional, local, and Tribal entities using BZPP funding in support of information sharing and intelligence fusion and analysis centers to leverage available Federal information sharing systems, including Law Enforcement Online (LEO) and the Homeland Security Information Network (HSIN). For additional information on LEO, contact the LEO Program Office at

[leoprogramoffice@leo.gov](mailto:leoprogramoffice@leo.gov) or (202) 324-8833. For additional information on HSIN and available technical assistance, contact the HSIN Help Desk at (703) 674-3003.