



U.S. DEPARTMENT OF HOMELAND SECURITY

**FISCAL YEAR 2009**

**BUFFER ZONE PROTECTION PROGRAM**

**GUIDANCE AND APPLICATION KIT**

**NOVEMBER 2008**



U.S. DEPARTMENT OF HOMELAND SECURITY

**Title of Opportunity:** FY 2009 Buffer Zone Protection Program

**Funding Opportunity Number:** DHS-09-GPD-078-1965

**Federal Agency Name:** FEMA Grant Programs Directorate (GPD)

**Announcement Type:** Initial

**Dates:** Completed applications must be submitted **no later than 11:59 PM EST, January 13, 2009.**

# CONTENTS

Contents.....	1
Part I. FUNDING OPPORTUNITY DESCRIPTION.....	2
Part II. AWARD INFORMATION .....	6
Part III. ELIGIBILITY INFORMATION .....	8
A.    Eligible Applicants.....	8
B.    Cost Sharing .....	10
C.    Restrictions .....	10
Part IV. APPLICATION AND SUBMISSION INFORMATION .....	11
A.    Address to Request Application Package .....	11
B.    Content and Form of Application .....	11
C.    Submission Dates and Times .....	15
D.    Intergovernmental Review .....	16
E.    Funding Restrictions.....	16
Part V. APPLICATION REVIEW INFORMATION .....	22
A.    Review Criteria.....	22
B.    Review Process .....	22
C.    Anticipated Announcement and Award Dates .....	22
Part VI. AWARD ADMINISTRATION INFORMATION .....	23
A.    Notice of Award .....	23
B.    Administrative and National Policy Requirements .....	23
C.    Reporting Requirements .....	30
Part VII. FEMA CONTACTS.....	34

## PART I.

# FUNDING OPPORTUNITY DESCRIPTION

The Buffer Zone Protection Program (BZPP) is one of five grant programs that constitute the Department of Homeland Security (DHS) Fiscal Year (FY) 2009 focus on infrastructure security activities. The BZPP 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 FY 2009 BZPP is authorized by the *Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009* (Public Law 110-329).

The vast majority 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.

### ***Federal Investment Strategy***

The BZPP is an important part of the Administration's larger, coordinated effort to strengthen homeland security preparedness, including the security of America's CIKR. The BZPP implements objectives addressed in a series of post 9/11 laws, strategy documents, plans and Homeland Security Presidential Directives (HSPDs). 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 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>1</sup> The Guidelines outline 15 scenarios of terrorist attacks or national disasters that form the basis of much of the Federal exercise and training

---

<sup>1</sup> The National Preparedness Guidelines and its supporting documents were published in September 2007. For purposes of aligning applications under the BZPP, applicants can rely on the finalized Guidelines, available at: <http://www.fema.gov/pdf/government/npg.pdf>.

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 continue to develop and implement a statewide and 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 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.

### ***BZPP Funding Priorities***

The FY 2009 BZPP 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<sup>2</sup> 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 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 (POCs) within these organizations
- Evaluating the capabilities of the responsible jurisdictions with respect to

---

<sup>2</sup> As used throughout this solicitation and regarding FY 2009 BZPP guidance, the term “responsible jurisdiction” shall refer to the primary agency, whether a State, local, or tribal entity or unit of government, as determined/approved by the State, that has authority over and around the identified CIKR facility, including the site’s adjacent grounds and/or structures.

planning for terrorism prevention and protection

- 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 2009 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 State and local jurisdictions to consider the following activities as priorities under the FY 2009 BZPP.

- 1. Coordination of Operational Activities with Public and Private Sector Partners.** DHS encourages that projects funded through the FY 2009 BZPP support coordination and direct interaction with private sector safety and security partners at the identified BZPP site. Examples include signing memorandums of understanding (MOUs) to allow facility security managers access to video camera surveillance feeds 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 2009 BZPP to support the 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 2009 BZPP support coordination and involvement of multidisciplinary partners in the development and implementation of preventive and protective measures, including emergency management and response, law enforcement, fire, public works, and public health personnel.
- 4. Strengthening IED Attack Prevention and Protection Capabilities.** DHS encourages that projects funded through the FY 2009 BZPP work to enhance capabilities to prevent and protect against terrorist use of Improvised Explosive Devices (IEDs). This priority aligns with the Homeland Security Grant Program guidance and the National Priority to Strengthen CBRNE Detection, Response, and Decontamination Capabilities, as outlined in the National Preparedness Guidelines. This priority supports the policy outlined in Homeland Security Presidential Directive 19 “Combating Terrorist Use of Explosives in the United States” (HSPD-19) by emphasizing the need for State and local jurisdictions to take an aggressive, coordinated, and proactive approach to reducing the threat of a terrorist explosive

attack. Examples include planning activities to implement multi-jurisdiction IED security plans or equipment that enhances the capabilities of bomb squads that serve the facility to diagnose and defeat IEDs.

- 5. Integration of Constellation/Automated Critical Asset Management System (C/ACAMS) and 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 in support of 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://preparednessportal.dhs.gov/>. Additional information on C/ACAMS is also available at <http://www.dhs.gov/acams>.

## PART II.

# AWARD INFORMATION

This section summarizes the award period of performance and the total amount of funding available under the FY 2009 BZPP, describes the basic distribution method used to determine final grant awards, and identifies all eligible applicants for FY 2009 BZPP funding.

### ***Award Period of Performance***

The period of performance of this grant is 36 months. 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.

### ***Available Funding***

In FY 2009, the total amount of funds distributed under the BZPP will be \$48,575,000. 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 DHS prioritization work with State and local stakeholders and partners, the following States, territories, and the District of Columbia are eligible to participate in, and receive funding under, the FY 2009 BZPP. 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. The available funding is summarized in Table 1 below.



**Table 1. FY 2009 BZPP Funding Allocations**

<b>State/Territory</b>	<b>Allocation</b>	<b>State/Territory</b>	<b>Allocation</b>
Alabama	\$400,000	Montana	\$400,000
Alaska	\$400,000	Nebraska	\$1,000,000
Arizona	\$400,000	Nevada	\$400,000
Arkansas	\$400,000	New Hampshire	\$200,000
California	\$5,200,000	New Jersey	\$3,600,000
Colorado	\$600,000	New Mexico	\$400,000
Connecticut	\$400,000	New York	\$4,787,500
Delaware	\$400,000	North Carolina	\$2,500,000
District of Columbia	\$600,000	North Dakota	\$200,000
Florida	\$800,000	Ohio	\$600,000
Georgia	\$600,000	Oklahoma	\$800,000
Hawaii	\$200,000	Oregon	\$400,000
Idaho	\$800,000	Pennsylvania	\$1,400,000
Illinois	\$3,000,000	Rhode Island	\$200,000
Indiana	\$1,000,000	South Carolina	\$400,000
Iowa	\$600,000	South Dakota	\$400,000
Kansas	\$600,000	Tennessee	\$1,887,500
Kentucky	\$400,000	Texas	\$4,200,000
Louisiana	\$1,200,000	U.S. Virgin Islands	\$200,000
Maine	\$200,000	Utah	\$200,000
Maryland	\$1,000,000	Virginia	\$600,000
Massachusetts	\$800,000	Washington	\$600,000
Michigan	\$800,000	West Virginia	\$600,000
Minnesota	\$200,000	Wisconsin	\$400,000
Mississippi	\$400,000	Wyoming	\$200,000
Missouri	\$600,000		
<b>Total</b>			<b>\$48,575,000</b>

## PART III.

# ELIGIBILITY INFORMATION

### A. Eligible Applicants

The Governor of each State has designated a State Administrative Agency (SAA) to apply for and administer the funds under the FY 2009 BZPP.<sup>3</sup> The SAA is the only agency eligible to apply for FY 2009 BZPP funds and is responsible for obligating the BZPP funds to the appropriate local units of government<sup>4</sup> or other designated recipients. The SAA must coordinate all BZPP activities with the respective State Homeland Security Advisor (HSA).

To be eligible to receive FY 2009 BZPP funding, applicants must meet NIMS compliance requirements. The NIMSCAST will be the required means to report FY 2008 NIMS compliance for FY 2009 preparedness award eligibility. All State and territory grantees were required to submit their compliance assessment via the NIMSCAST by September 30, 2008 in order to be eligible for FY 2009 preparedness programs. The State or territory department/agency grantee reserves the right to determine compliance reporting requirements of their sub-awardees (locals) in order to disperse funds at the local level.

For FY 2009 there are no new NIMS compliance objectives. If FY 2008 NIMS compliance was reported using NIMSCAST and the grantee has met all NIMS compliance requirements, then NIMSCAST will only require an update in FY 2009. Additional information on achieving compliance is available through the FEMA National Integration Center (NIC) at <http://www.fema.gov/emergency/nims/>.

The risk methodology for the FY 2009 BZPP is consistent across the infrastructure security activities 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

---

<sup>3</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." 6 U.S.C. § 101.

<sup>4</sup> As defined in the House Report (H. Rept. 110-862, p. 115) and the Senate Report (S. Rept. 110-396, p. 109) accompanying the *Consolidated Security, Disaster Assistance, and Continuing Appropriations Act of 2009* (Public Law 110-329), 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."

DHS with the ability to focus the allocation of BZPP resources to those jurisdictions responsible for the highest risk sites.

Based on risk, all BZPP sites have been selected prior to the grant announcement. Therefore, FY 2009 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 high-risk sites that are close in proximity to one another. DHS will work closely with these States and provide supplemental guidance for these strategic projects within the FY 2009 BZPP timelines to ensure coordinated planning<sup>5</sup>.

Through the FY 2009 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:

- Highest consequence chemical facilities
- Nuclear power plants
- Higher consequence liquefied 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

### ***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>6</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

---

<sup>5</sup> In the course of closing gaps at sites specifically identified by DHS in the 2009 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 submit a justification to reallocate the residual funds to an alternative Tier 1 or 2 CIKR site to DHS for approval.

<sup>6</sup> DHS is increasingly leveraging a common risk model as outlined in the NIPP Base Plan to provide a systematic and comparable estimate of risk that can help inform national and sector-level risk management decisions. This model is maturing and it is expected that new risks will be identified as more assets and systems are assessed.

- Severe national security impacts

DHS worked with the Sector Specific Agencies (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 2009 BZPP, include:

- Sites that have successfully enhanced their prevention and protection posture by reducing their exposure to the risk of a terrorist attack through prior BZPP grant funding
- Sites eligible for funding through the Homeland Security Grant Program (HSGP) and/or other grant program funding that more directly addresses risks associated with the specific site

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 based on risk, and funds are being systematically applied to address the list of assets supported by the BZPP. 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.

**Note: FY 2009 BZPP materials and site lists may not be distributed to anyone outside those entities working in an official capacity to manage, develop, and implement the BZPP at the identified sites. All BZPP generated materials must also be clearly labeled and distributed according to the requirements listed in the FY 2009 BZPP Guidance and Application Kit.**

## **B. Cost Sharing**

There is no required cost sharing, matching, or cost participation for the FY 2009 BZPP.

## **C. Restrictions**

Please see Part IV.E. for Management & Administration (M&A) limits and allowable/unallowable costs guidance.

PART IV.  
**APPLICATION AND SUBMISSION  
INFORMATION**

**A. Address to Request Application Package**

DHS participates in the Administration's e-government initiative. As part of that initiative, all applications must be filed 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>. To access application forms and instructions, select "Apply for Grants," and then select "Download Application Package." Enter the CFDA and/or the funding opportunity number located on the cover of this announcement. Select "Download Application Package," and then follow the prompts to download the application package. To download the instructions, go to "Download Application Package" and select "Instructions." If you experience difficulties or have any questions, please call the [grants.gov](http://www.grants.gov) customer support hotline at (800) 518-4726.

**B. Content and Form of Application**

**1. On-line application.** The on-line application must be completed and submitted using [grants.gov](http://www.grants.gov) after Central Contractor Registry (CCR) registration is confirmed. The on-line application includes the following required forms and submissions:

- Standard Form 424, Application for Federal Assistance
- Standard Form 424A, Budget Information
- Standard Form 424B, Assurances
- Standard Form LLL, Disclosure of Lobbying Activities

The program title listed in the Catalog of Federal Domestic Assistance (CFDA) is "*Buffer Zone Protection Program*." The CFDA number is **97.078**. When completing the on-line application, applicants should identify their submissions as new, non-construction applications.

**2. Application via [grants.gov](http://www.grants.gov).** FEMA 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>.

**3. 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 (866) 705-5711.

4. **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).
5. **Buffer Zone Plans (BZPs) and Vulnerability Reduction Purchasing Plans (VRPPs).** The Office of Infrastructure Protection (IP), Protective Security Coordination Division (PSCD) provides a range of support to BZPP grantees and sub-grantees. The 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 development 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 comprehensive 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 in support of coordinated prevention and protection efforts of CIKR.

- The responsible jurisdiction is required to notify and include their Protective Security Advisor (PSA) 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. The responsible jurisdiction is 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 jurisdiction is 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 jurisdiction 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 is 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, and/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 jurisdiction 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 jurisdiction 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 [ipassessments@dhs.gov](mailto:ipassessments@dhs.gov).

***BZPP Coordination Requirements***

Use of FY 2009 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 HSA, as well as any applicable State strategy planning teams, UAWGs, RTSWGs, and/or AMSCs, as applicable.

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 other grant 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.

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.
3. **Urban Area Working Group (UAWG) Coordination.** Each identified Urban Areas Security Initiative (UASI) geographical area is governed by an UAWG. The UAWG is composed of multidiscipline and multijurisdictional 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. The responsible jurisdiction must coordinate the development and implementation of the BZP and VRPP with any UAWGs, as applicable to the geographic area, to ensure all programs, plans, and requested resources are coordinated and leveraged across the region.
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' mission to protect CIKR by fostering improved coordination at the State and local level through their support for national CIKR protection-related programs. The responsible jurisdiction must coordinate with and include their PSA in the assessment of CIKR identified for BZPP funding to ensure all necessary resources are made available for the development of the BZP.

#### ***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 Protected Critical Infrastructure Information (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) unless the documents are submitted using the Automated Critical Asset Management System (ACAMS) tool. Any submissions utilizing the ACAMS tool should be submitted in the Adobe PDF format. If PCII protection is not requested, the Express and Certification statements **must** be removed from the BZP template prior to submission.

- The BZPs and VRPPs must be submitted electronically via *the FEMA Preparedness Portal* located at: <https://preparednessportal.dhs.gov/>. The SAA must submit the BZP and VRPP for each site into the individual FY 2009 State folder provided for DHS approval by **November 30, 2009**. **If States fail to submit all BZPP materials by this date, the requirements of the grant have not been met, and necessary steps may be taken by DHS to deobligate funds.**
- 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 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 resubmissions **must** contain updated, complete versions of **both** the BZP and VRPP and appropriately identify whether PCII protection is requested. **Any submissions that fail to follow any of the guidelines above will neither be accepted nor reviewed.**
- 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 2009 BZPP may not be obligated, drawn down, or disbursed 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.

### C. Submission Dates and Times

Completed applications must be submitted electronically through [www.grants.gov](http://www.grants.gov) **no later than 11:59 PM EST, January 13, 2009**. Late applications will neither be considered nor reviewed. Upon successful submission, a confirmation e-mail message will be sent with a [grants.gov](http://www.grants.gov) tracking number, which is needed to track the status of the application.

The SAA must submit the BZP and VRPP for each site to DHS for approval by **November 30, 2009**. **If States fail to submit all BZPP materials by this date, requirements of the grant have not been met, and necessary steps may be taken by DHS to deobligate funds.**

#### **D. Intergovernmental 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 Single Point of Contact (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>. *The names and addresses of the SPOCs are listed on OMB's home page, available at: <http://www.whitehouse.gov/omb/grants/spoc.html>.*

#### **E. Funding Restrictions**

The applicable SAAs will be responsible for administration of the FY 2009 BZPP. In administering the program, the SAA must work with eligible applicants to comply with the following general requirements:

- 1. 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.

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 2009 BZPP.
  - To assist with the coordination and implementation requirements of the FY 2009 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 2009 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 2009 BZPP.

**2. Allowable Costs.** FY 2009 BZPP allowable costs are divided into the following categories:

- Planning
- Equipment acquisition

This section provides guidance on the types of expenditures that are allowable under the FY 2009 BZPP. Grantees are encouraged to contact their FEMA Program Analyst regarding authorized and unauthorized expenditures.

### ***Planning***

Planning activities are central to the implementation of the FY 2009 BZPP, which 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 multidiscipline 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 State and local homeland security partners to determine additional funding source opportunities for planning-related purposes (such as FEMA's Homeland Security Grant Program).

FY 2009 BZPP funds may be used for a range of homeland security and CIKR protection planning activities, such as:

- **Developing and implementing homeland security and CIKR support programs and adopting DHS national initiatives limited to the following:**
  - Implementing the National Preparedness Guidelines, as they relate to implementation of the NIPP and SSPs.
  - Building or enhancing preventive radiological and nuclear detection programs.
  - 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 National Integration Center (NIC).

- Designing State and local geospatial data systems.
- **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, advanced warning of a possible terrorist incident, 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.
  - Developing and implementing CIKR capabilities within fusion centers and/or intelligence units, in accordance with the forthcoming *Critical Infrastructure and Key Resource Protection Capabilities for Fusion Centers*<sup>7</sup>
  - Developing and implementing liaison officer programs to share CIKR information with fusion centers and/or intelligence units.
  - 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.
- **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.

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).

### ***Equipment***

FY 2009 BZPP funds may be used for the following categories of equipment. A comprehensive listing of allowable equipment categories and types is found on the web-based Authorized Equipment List (AEL) on the Responder Knowledge Base (RKB) at <https://www.rkb.us/lists.cfm>.

The Standardized Equipment List (SEL) is located at this site as well. In some cases, items on the SEL are not allowable under BZPP or will not be eligible for purchase

---

<sup>7</sup> An Appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers*

unless specific conditions are met. Unless otherwise stated, equipment must meet all mandatory regulatory and/or DHS-adopted standards to be eligible for purchase using these funds. In addition, agencies will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment.

**Table 2. BZPP Allowable Equipment Categories**

#	Category Title
[2]	Explosive Device Mitigation and Remediation Equipment <sup>8</sup>
[3]	CBRNE Operational Search and Rescue Equipment <sup>9</sup>
[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 <sup>9</sup>

Other specialized equipment not listed within 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 Program Analyst, 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 2009 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).

<sup>8</sup> Requests for equipment to support Explosive Device Response Operations must indicate within the Notes section of the VRPP the name of the FBI accredited bomb squad or prospective bomb squad that is undergoing the accreditation process that will be receiving and utilizing the requested equipment.

<sup>9</sup> Only select sub-categories within AEL Category 3 and 20 are eligible for FY 2009 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.

- Address a specific threat, vulnerability, and/or consequence directly related to a heightened alert period, as related to the site and/or its sector.

**3. Unallowable Costs.** The following projects and costs are considered **ineligible** for award consideration:

- **Hiring of Public Safety Personnel.** FY 2009 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/or renovation is prohibited under the FY 2009 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 2009 BZPP site is a federal facility, the FY 2009 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 2009 BZPP activities.
- **Training and Exercise Activities.** Any resulting training or exercise requirements identified through the BZPP may not be funded with FY 2009 BZPP funds, but may be funded through other overarching homeland security grant programs (e.g., State Homeland Security Grant Program and Urban Areas Security Initiative) 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 FY 2009 BZPP, items not in accordance with the AEL, or previously identified as ineligible within this guidance, are not an allowable cost.

## PART V.

# APPLICATION REVIEW INFORMATION

### A. Review Criteria

This section summarizes the core process and priorities used to assess applications under the FY 2009 BZPP. The FY 2009 BZPP used risk-based formula funding consistent with FEMA policy outlined in this guidance document. Each applicant's final funding allocation is determined through the use of risk analyses.

Applications will be evaluated through a Federal review process for completeness, adherence to programmatic guidelines, feasibility, and how well the proposed VRPP expenditures address the identified need(s), vulnerabilities, or capability shortfall(s). The VRPP requires narrative on overall strategic alignment with State Homeland Security Strategies and the NIPP, impact and sustainability, and support for the national priorities and target capabilities. These criteria will be used to evaluate the anticipated effectiveness of all proposed expenditures.

### B. Review Process

The following process will be used to provide final approval to BZP and VRPPs submitted under the FY 2009 BZPP:

- FEMA will verify compliance with all administrative and eligibility criteria identified in the application kit.
- IP will provide a technical review via subject matter expert to ensure all of the identified need(s), vulnerabilities, or capability shortfall(s) have been addressed.
- FEMA will evaluate the narrative provided within the VRPP for overall strategic alignment with State Homeland Security Strategies and the NIPP, impact and sustainability, support for the national priorities and target capabilities, and equipment allowability.

### C. Anticipated Announcement and Award Dates

FEMA will evaluate and act on applications within 60 days following close of the application period, consistent with the *Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009* (Public Law 110-329). Awards will be made on or before September 30, 2009.



## PART VI.

# AWARD ADMINISTRATION INFORMATION

### A. Notice of Award

Upon approval of an application, the grant will be awarded to the grant recipient. The date that this is done is the “award date.” Notification of award approval is made through the Grants Management System (GMS). Once an award has been approved, a notice is sent to the authorized grantee official. Follow the directions in the notification 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, please contact your Program Analyst 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.

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. Administrative and National Policy Requirements

1. **State Preparedness Report.** The *Post-Katrina Emergency Management Reform Act of 2006* (Public Law 109-295) requires any State that receives Federal preparedness assistance to submit a State Preparedness Report to DHS. FEMA will provide additional guidance on the requirements for updating State Preparedness Reports. **Receipt of this report is a prerequisite for applicants to receive any FY 2009 DHS preparedness grant funding.**
2. **Standard Financial Requirements.** The grantee and any subgrantee shall comply with all applicable laws and regulations. A non-exclusive list of regulations commonly applicable to DHS grants are listed below:
  - 2.1 -- **Administrative Requirements.**
    - 44 CFR Part 13, Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments
    - 2 CFR Part 215, Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations (OMB Circular A-110)

## **2.2 -- Cost Principles.**

- 2 CFR Part 225, Cost Principles for State, Local, and Indian Tribal Governments (OMB Circular A-87)
- 2 CFR Part 220, Cost Principles for Educational Institutions (OMB Circular A-21)
- 2 CFR Part 230, Cost Principles for Non-Profit Organizations (OMB Circular A-122)
- Federal Acquisition Regulations (FAR), Part 31.2 Contract Cost Principles and Procedures, Contracts with Commercial Organizations

## **2.3-- Audit Requirements.**

- OMB Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations

**2.4 -- Duplication of Benefits.** There may not be a duplication of any federal assistance, per A-87, Basic Guidelines Section C.3 (c), which states: Any cost allocable to a particular Federal award or cost objective under the principles provided for in this Circular may not be charged to other Federal awards to overcome fund deficiencies, to avoid restrictions imposed by law or terms of the Federal awards, or for other reasons. However, this prohibition would not preclude governmental units from shifting costs that are allowable under two or more awards in accordance with existing program agreements.

**3. Non-supplanting Requirement.** 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.

## **4. Technology Requirements.**

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

**4.2 -- 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). FEMA encourages grantees to align any geospatial activities with the guidance available on the FEMA website at <http://www.fema.gov/grants>.

**4.3 -- 28 CFR Part 23 guidance.** FEMA requires that any information technology system funded or supported by these funds comply with 28 CFR Part

23, Criminal Intelligence Systems Operating Policies, if this regulation is determined to be applicable.

## **5. Administrative Requirements.**

**5.1 -- Freedom of Information Act (FOIA).** FEMA 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 FEMA 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.

**5.2 -- Protected Critical Infrastructure Information (PCII).** The PCII Program, established pursuant to the *Critical Infrastructure Information Act of 2002* (Public Law 107-296) (CII Act), created a new framework, which enables State and local jurisdictions and members of the private sector to voluntarily 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 a 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 a memorandum of agreement (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).

**5.3 -- 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.

**5.4 -- Services to limited English proficient (LEP) persons.** Recipients of FEMA 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 proposals and budgets and in conducting their programs and activities. Reasonable costs associated with providing meaningful access for LEP individuals are considered allowable program costs. For additional information, see <http://www.lep.gov>.

**5.5 -- 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 FEMA. In addition, Executive Order 13347, *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 encourage consideration of the needs of individuals with disabilities served by State, local, and tribal governments in emergency preparedness planning.

FEMA 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:

- **Comprehensive Preparedness Guide 301 (CPG-301): Interim Emergency Management Planning Guide for Special Needs Populations:** CPG-301 is designed to aid tribal, State, territorial, and local governments in planning for individuals with special needs. CPG-301 outlines special needs considerations for: Developing Informed Plans; Assessments and Registries; Emergency Public Information/Communication; Sheltering and Mass Care; Evacuation; Transportation; Human Services/Medical Management; Congregate Settings; Recovery; and Training and Exercises. CPG-301 is available at <http://www.fema.gov/pdf/media/2008/301.pdf>.
- **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 Federal, State, and local 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.

**5.6 -- Compliance with the National Energy Conservation Policy and Energy Policy Acts.** In accordance with the *Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009* (Public Law 110-329), grant funds must comply with the following two requirements:

- None of the funds made available shall be used in contravention of the Federal buildings performance and reporting requirements of Executive Order 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).

**5.7 -- 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 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 these 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.

Recipient shall not undertake any project having the potential to impact EHP resources without the prior approval of FEMA, including but not limited to communications towers, physical security enhancements, new construction, and **modifications to buildings, structures and objects** that are 50 years old or greater. Recipient must comply with all conditions placed on the project as the result of the EHP review. Any change to the approved project scope of work will require re-evaluation for compliance with these EHP requirements. If ground disturbing activities occur during project implementation, the recipient must ensure monitoring of ground disturbance, and if any potential archeological resources are discovered, the recipient will immediately cease construction in that area and notify FEMA and the appropriate State Historic Preservation Office. **Any construction activities that have been initiated without the necessary EHP review and approval will result in a non-compliance finding and will not be eligible for FEMA 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*, available at <http://ojp.usdoj.gov/odp/docs/info271.pdf>. Additional information and resources can also be found at <http://www.fema.gov/plan/ehp/ehp-applicant-help.shtm>.

**5.8 -- Royalty-free License.** Applicants are advised that FEMA reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, or otherwise use, and authorize others to use, for Federal government purposes: (a) the copyright in any work developed under an award or sub-award; and (b) any rights of copyright to which an award recipient or sub-recipient purchases ownership with Federal support. Award recipients must agree to consult with

FEMA regarding the allocation of any patent rights that arise from, or are purchased with, this funding.

**5.9 -- Publications Statement.** Applicants are advised that all publications created with funding under any grant award shall prominently contain the following statement: "This document was prepared under a grant from FEMA's Grant Programs Directorate, U.S. Department of Homeland Security. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position or policies of FEMA's Grant Programs Directorate or the U.S. Department of Homeland Security."

**5.10 -- Equipment Marking.** Applicants are advised that, when practicable, any equipment purchased with grant funding shall be prominently marked as follows: "Purchased with funds provided by the U.S. Department of Homeland Security."

**5.11 -- Disadvantaged Business Requirement.** Applicants are advised that, to the extent that recipients of a grant use contractors or subcontractors, such recipients shall use small, minority, women-owned or disadvantaged business concerns and contractors or subcontractors to the extent practicable.

**5.12 -- National Preparedness Reporting Compliance.** *The Government Performance and Results Act (Public Law 103-62) (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. FEMA anticipates using this information to inform future-year grant program funding decisions. Award recipients must agree to cooperate with any assessments, national evaluation efforts, or information or data collection requests, including, but not limited to, the provision of any information required for the assessment or evaluation of any activities within their grant agreement. This includes any assessments, audits, or investigations conducted by the Department of Homeland Security, Office of the Inspector General, or the Government Accountability Office.

## **C. 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 the FEMA Payment and Reporting System (PARS) contains edits that will prevent access to funds if reporting requirements are not met on a timely basis.

- 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.

Reporting periods and due dates:

- October 1 – December 31; *Due January 30*
- January 1 – March 31; *Due April 30*
- April 1 – June 30; *Due July 30*
- July 1 – September 30; *Due October 30*

- 2. Categorical Assistance Progress Report (CAPR).** Following an award, the awardees 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 reports. Awardees should include a statement in the narrative field of the CAPR that reads: *See BSIR.*

The CAPR is due within 30 days after the end of the reporting period (July 30 for the reporting period of January 1 through June 30; and January 30 for the reporting period of July 1 though December 31). Future awards and fund drawdowns may be withheld if these reports are delinquent.

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

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

- 3. Initial Strategy Implementation Plan (ISIP).** Following an award, the awardees will be responsible for providing updated obligation and expenditure information to meet the pass-through requirement. The applicable SAAs are responsible for completing and submitting the ISIP online.

***Required submission: ISIP (due within 45 days of award date)***

- 4. Biannual Strategy Implementation Reports (BSIR).** Following an award, the awardees 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 BSIR report which is a component of the CAPR. The BSIR submission will satisfy the narrative requirement of the CAPR. SAAs are still required to submit the CAPR with a statement in the narrative field that reads: *See BSIR.*

The BSIR is due within 30 days after the end of the reporting period (July 30 for the reporting period of January 1 through June 30; and 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.

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

- 5. 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 FY 2009 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.

***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. Programmatic monitoring may also include the Regional Federal Preparedness Coordinators, when appropriate, to ensure consistency of project investments with Regional and National goals and policies, as well as to help synchronize similar investments ongoing at the Federal, State, and local levels.

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.

***Grant Close-Out Process***

Within 90 days after the end of the period of performance, grantees 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 close-out notice will be completed to close out the grant. The notice will indicate the project as 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. The grantee is responsible for returning any funds that have been drawdown but remain as unliquidated on grantee financial records.

***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.***

## PART VII.

# FEMA CONTACTS

This section describes several resources that may help applicants in completing a FEMA grant application. During the application period FEMA will identify multiple opportunities for a cooperative dialogue between the Department and applicants. This commitment is intended to ensure a common understanding of the funding priorities and administrative requirements associated with the FY 2009 BZPP, and to help in submission of projects that will have the highest impact on reducing risks.

- 1. Centralized Scheduling & Information Desk (CSID) Help Line.** 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. CSID provides general information on all FEMA grant programs and information on the characteristics of CBRNE, agro-terrorism, defensive equipment, mitigation techniques, and available Federal assets and resources.

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. 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. Additional guidance and information can be obtained by contacting the FEMA Call Center at (866) 927-5646 or via e-mail to [ASK-GMD@dhs.gov](mailto:ASK-GMD@dhs.gov).
- 3. GSA's State and Local Purchasing Programs.** 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  
Cooperative Purchasing, authorized by statute, allows State and local governments to purchase a variety of supplies (products) and services under



specific GSA Schedule contracts to save time, money, and meet their everyday needs and missions.

The Cooperative Purchasing program allows State and local governments to purchase alarm and signal systems, facility management systems, firefighting and rescue equipment, law enforcement and security equipment, marine craft and related equipment, special purpose clothing, and related services off of Schedule 84 and Information Technology products and professional services off of Schedule 70 and the Consolidated Schedule (containing IT Special Item Numbers) **only**. Cooperative Purchasing for these categories is authorized under Federal law by the *Local Preparedness Acquisition Act* (Public Law 110-248) and Section 211 of the *E-Government Act of 2002* (Public Law 107-347).

Under this program, State and local governments have access to 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 GSA to provide State and Local governments the use of ALL GSA Federal Supply Schedules 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*. 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 contractors on GSA's website, <http://www.gsaelibrary.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/csd> to find a local customer service director in your area. For assistance at the national level, contact Tricia Reed at [tricia.reed@gsa.gov](mailto:tricia.reed@gsa.gov), (571) 259-9921. More information is available on all GSA State and local programs at: [www.gsa.gov/stateandlocal](http://www.gsa.gov/stateandlocal).

#### **4. Homeland Security Preparedness Technical Assistance Program.** The Homeland Security Preparedness Technical Assistance Program (HSPTAP)

provides direct support 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 prevent, protect against, respond to, and recover from terrorist and all hazard threats. In addition to the risk assessment assistance already being provided, FEMA also offers a variety of other direct support assistance programs.

More information can be found at [http://www.fema.gov/about/divisions/pppa\\_ta.shtm](http://www.fema.gov/about/divisions/pppa_ta.shtm).

- 5. 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 homeland security officials, as well as an updated list of homeland security exercises, events, and conferences. Additionally, LLIS includes online collaboration tools, including secure email 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>.

- 6. Information Sharing Systems.** FEMA encourages all State, regional, local, and tribal entities using FY 2009 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.