U.S. DEPARTMENT OF HOMELAND SECURITY

Fiscal Year 2008

URBAN AREAS SECURITY INITIATIVE NONPROFIT SECURITY GRANT PROGRAM

GUIDANCE AND APPLICATION KIT

February 2008

CONTENTS

PART I.
INTRODUCTION

The Fiscal Year (FY) 2008 Urban Areas Security Initiative (UASI) Nonprofit Security Grant Program (NSGP) provides funding support for target hardening activities to nonprofit organizations that are at high risk of international terrorist attack. While this funding is provided specifically to high-risk nonprofit organizations, the program seeks to integrate nonprofit preparedness activities with broader state and local preparedness efforts. It is also designed to promote coordination and collaboration in emergency preparedness activities among public and private community representatives, State and local government agencies, and Citizen Corps Councils.

PART II.
FUNDING AVAILABILITY AND ELIGIBLE APPLICANTS

A.   Funding Availability

The UASI Nonprofit Security Grant Program will provide $15 million to high-risk nonprofit organizations. Each nonprofit organization may apply through their State for up to a $75,000 grant award.

B.   Eligible Applicants

The Governor of each State and Territory with an eligible FY 2008 Urban Area Security Initiative (UASI) jurisdiction is required to designate a State Administrative Agency (SAA) to apply for and administer the funds awarded under the UASI Nonprofit Security Grant Program. The SAA is the only entity eligible formally to apply for these funds. Applications must be provided to the SAA from eligible nonprofit organizations (as described under section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from tax under section 501(a) of such Code) that are at **high risk of international terrorist attack** and are located within one of the specific UASI-eligible Urban Areas listed in Table 1.

SAAs, in coordination with Urban Area Working Groups and the Citizen Corps Councils, are encouraged to actively and aggressively advertise the availability of the Nonprofit Security Grant Program (NSGP) to eligible non-profit organizations, especially to organizations that previously have not applied for or received NSGP funding. This is not meant to imply that previous recipients are ineligible to apply for FY 2008 funds, but FEMA would like to ensure that the NSGP is advertised widely and ALL eligible applicants are afforded a reasonable opportunity to obtain funding.

Criteria for determining eligible applicants who are at high risk of terrorist attack include, but are not limited to:

- Identification and substantiation (e.g. police reports or insurance claims) of prior threats or attacks against the nonprofit organization or closely related organizations (within or outside the U.S.) by a terrorist organization, network, or cell
- Symbolic value of the site(s) as a highly recognized national or historical institution that renders the site a possible target of international terrorism
- Role of the applicant nonprofit organization in responding to or recovering from international terrorist attacks
- Findings from previously conducted risk assessments including threat or vulnerability

Table 1 – Eligible Urban Areas under the FY 2008 UASI Program

FY 2008 Tier I Urban Areas*			
(CA)	Los Angeles/Long Beach Area	(NJ)	Jersey City/Newark Area
(CA)	Bay Area	(NY)	New York City Area
(DC)	National Capital Region	(TX)	Houston Area
(IL)	Chicago Area		

FY 2008 Tier II Urban Areas*			
(AZ)	Phoenix Area	(NV)	Las Vegas Area
(AZ)	Tucson Area	(NY)	Albany Area
(CA)	Riverside Area	(NY)	Buffalo Area
(CA)	Sacramento Area	(NY)	Rochester Area
(CA)	San Diego Area	(NY)	Syracuse Area
(CA)	Anaheim/Santa Ana Area	(OH)	Cincinnati Area
(CO)	Denver Area	(OH)	Cleveland Area
(CT)	Bridgeport Area	(OH)	Columbus Area
(CT)	Hartford Area	(OH)	Toledo Area
(FL)	Fort Lauderdale Area	(OK)	Oklahoma City Area
(FL)	Jacksonville Area	(OR)	Portland Area
(FL)	Miami Area	(PA)	Philadelphia Area
(FL)	Orlando Area	(PA)	Pittsburgh Area
(FL)	Tampa Area	(PR)	San Juan Area
(GA)	Atlanta Area	(RI)	Providence Area
(HI)	Honolulu Area	(TN)	Memphis Area
(IN)	Indianapolis Area	(TN)	Nashville Area
(KY)	Louisville Area	(TX)	Austin Area
(LA)	Baton Rouge Area	(TX)	Dallas/Fort Worth/Arlington Area
(LA)	New Orleans Area	(TX)	El Paso Area
(MA)	Boston Area	(TX)	San Antonio Area
(MD)	Baltimore Area	(UT)	Salt Lake City Area
(MI)	Detroit Area	(VA)	Richmond Area
(MN)	Twin Cities Area	(VA)	Norfolk Area
(MO)	Kansas City Area	(WA)	Seattle Area
(MO)	St. Louis Area	(WI)	Milwaukee Area
(NC)	Charlotte Area		

✱ Alphabetical placement does not equate to funding allocation.

<div align="center">

PART **III.**
PROGRAM REQUIREMENTS

</div>

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

A. General Program Requirements

The SAA is the only entity eligible formally to apply for these funds. Applications must be provided to the SAA from eligible nonprofit organizations (as described under section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from tax under section 501(a) of such Code) that are at **high risk of international terrorist attack** and are located within one of the specific UASI-eligible urban areas listed in Table 1.

Grant funds. States must pass-through at a minimum, 97 percent of NSGP grant funds. Any funds retained by the State on behalf of NSGP for management and administrative purposes must be used in direct support of the NSGP jurisdiction. States must provide documentation, upon request from the NSGP jurisdiction, demonstrating how any NSGP funds retained by the State are directly supporting the 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 NSGP award. States may pass through a portion of the State M&A allocation to local subgrantees to support local management and administration activities.

Match requirement. Grant recipients must meet a 75 percent Federal-25 percent grantee match requirement. Grantee contributions must be from non-Federal sources. The grantee's match may be met through cash or in-kind contributions which may include training investments related to use of equipment purchased with the grant, or training investments related to general purpose security and emergency preparedness for staff. For example, the costs of training security guards on new screening equipment purchased as part of the grant or providing general preparedness training for nonprofit organization staff can be leveraged to satisfy the match. In no event can regular personnel costs such as salary, overtime, or other operational costs unrelated to training be used to satisfy the matching requirement.

B. Application Requirements

The following steps must be completed using the on-line *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.

Applicants must complete the following for the FY 2008 UASI Nonprofit Security Grant Program application:

❑	Valid Central Contractor Registry (CCR) Registration
❑	Data Universal Numbering System (DUNS) Number
❑	*Grants.gov* Online Application
❑	Review of Application by the State Single Point of Contact (SPOC) (*if applicable*)
❑	Investment Justifications for all nonprofit organization applicants in PDF format
❑	List of all prioritized scores assigned to each nonprofit organization investment justification, in accordance with the "*Investment Justification Questions, Criteria, and Prioritization Methodology for SAAs and Urban Area Working Groups*" excel template

Note: In addition to these general requirements, applicants should review the relevant program-specific sections of this Guidance for additional requirements. *All grant recipients are assumed to have read, understood, and accepted the Program Guidance as binding.*

1. **Application via *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*. Eligible SAAs must apply for funding through this portal, accessible on the Internet at *http://www.grants.gov*.

2. **Application deadline**. Completed Applications must be submitted to *grants.gov* no later than **11:59 PM EDT, May 1, 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.*

4. **On-line application.** The on-line application must be completed and submitted using *grants.gov* after CCR registration is confirmed. The on-line application includes the following required forms and submissions:
   - Standard Form 424, Application for Federal Assistance

- Standard Form 424B Assurances
- Standard Form LLL, Disclosure of Lobbying Activities
- Standard Form 424A, Budget Information
- Certification Regarding Debarment, Suspension, and Other Responsibility Matters
- Any additional Required Attachments

The program title listed in the Catalog of Federal Domestic Assistance (CFDA) is "*Homeland Security Grant Program.*" The CFDA number is **97.008**. 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 24 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 SAA and nonprofit applicants must each provide a Dun and Bradstreet Data Universal Numbering System (DUNS) number with their application. This number is a required field within *grants.gov* for CCR Registration and within the Investment Justification. 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 (800) 333-0505.

7. **Investment Justifications.** As part of the application process, applicants must develop a formal Investment Justification that addresses each initiative being proposed for funding.

   Please see Appendix A as well for further guidance in preparing the Investment Justification.

8. **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.

9. **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*.

10. **Standard financial requirements.**

   10.1 -- Non-supplanting certification. This certification affirms that grant funds will be used to supplement existing funds, and will not replace (supplant) funds that have been appropriated for the same purpose. Applicants or grantees may be required to supply documentation certifying that a reduction in non-Federal resources occurred for reasons other than the receipt or expected receipt of Federal funds.

   10.2 -- Assurances. Assurances forms (SF-424B and SF-424D) can be accessed at *http://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.

   10.3 -- 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_00/44cfrv1_00.html*.

11. **Technology requirements.**

   11.1 -- 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 NSGP awards. Further information about the required use of NIEM specifications and guidelines is available at *http://www.niem.gov*.

   11.2 -- Geospatial guidance. Geospatial technologies capture, store, analyze, transmit, and/or display location-based information (i.e., information that can be

linked to a latitude and longitude). DHS encourages grantees to align any geospatial activities with the guidance available on the FEMA website at *http://www.fema.gov/grants*.

11.3 -- 28 CFR Part 23 guidance. DHS requires that any information technology system funded or supported by NSGP funds comply with 28 CFR Part 23, Criminal Intelligence Systems Operating Policies, if this regulation is determined to be applicable.

12.   Administrative requirements.

12.1 -- Freedom of Information Act (FOIA). DHS recognizes that much of the information submitted in the course of applying for funding under this program or provided in the course of its grant management activities may be considered law enforcement sensitive or otherwise important to national security interests. 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.

12.2 -- Protected Critical Infrastructure Information (PCII). The PCII Program, established pursuant to the Critical Infrastructure Information Act of 2002 (CII Act), created a new framework, which enables State and local jurisdictions and members of the private sector voluntarily to submit sensitive information regarding critical infrastructure to DHS. The Act also provides statutory protection for voluntarily shared CII from public disclosure and civil litigation. If validated as 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.

12.3 -- Compliance with Federal civil rights laws and regulations. The grantee is required to comply with Federal civil rights laws and regulations. Specifically, the grantee is required to provide assurances as a condition for receipt of Federal 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.

12.4 -- Services to limited English proficient (LEP) persons. Recipients of DHS financial assistance are required to comply with several Federal civil rights laws, including Title VI of the Civil Rights Act of 1964, as amended. These laws prohibit discrimination on the basis of race, color, religion, 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*.

12.5 -- 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/oer/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.

12.6 -- 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).

12.7 -- 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 NSGP 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.*

C. Application Evaluation

DHS will evaluate and act on applications within **90 days** of the submission deadline. Each Investment Justification will be reviewed for completeness, adherence to programmatic guidelines, feasibility, and how well the proposed solution addresses the identified risk. Applications will be reviewed in two phases to leverage local knowledge and understanding of the applicant's risk for terrorist attack, while also ensuring coordination and alignment with Federal, State and local preparedness efforts.

First, applications will be reviewed and prioritized by the respective Urban Area Working Group (UAWG) in coordination with the local Citizen Corps Council, if they are separate entities. The UAWG is responsible for coordinating the development and implementation of all preparedness activities for its respective local jurisdictions. Prioritized applications will be reviewed by the respective State Administrative Agency (SAA) for concurrence/non-concurrence. As part of the UASI Nonprofit Security Grant Program application, the SAA must work with the UAWG and local Citizen Corps Council to develop a prioritized list of nonprofit proposals, in accordance with the "*Investment Justification Questions, Criteria, and Prioritization Methodology for SAAs and UAWGs"* excel template located at *http://www.fema.gov/grants.* This list and all investment justifications will be submitted through grants.gov. Finally applications will be reviewed and award determinations made through a panel of evaluators from across DHS, including components within the Federal Emergency Management Agency, the Office of Infrastructure Protection (e.g., Protective Security Coordination Division, Office of Bombing Prevention), the Domestic Nuclear Detection Office (as applicable), and the Office of Intelligence and Analysis.

Evaluation criteria include items such as:

- Identification and substantiation of prior threats or attacks (within or outside the U.S.) by a terrorist organization, network, or cell against the applicant
- Symbolic value of the site(s) as a highly recognized national or historical institution that renders the site a possible target of terrorism
- Proximity of the nonprofit organization to identified CI/KR
- Role of the applicant nonprofit organization in responding to terrorist attacks
- Findings from previously conducted threat and/or vulnerability assessments
- Integration of nonprofit preparedness with broader state and local preparedness efforts to include coordination with the Citizen Corps Council
- Complete, feasible investment justifications that address an identified risk, including threat and vulnerability

D.   Allowable Costs Guidance

1. Equipment. Allowable costs are focused on target hardening activities. Thus, funding can be used for the acquisition and installation of security equipment on real property (including buildings and improvements) owned or leased by the nonprofit organization, specifically in prevention of and/or protection against the risk of a terrorist attack. This equipment is **limited to two categories** of items on the Authorized Equipment List (AEL):

- Physical Security Enhancement Equipment
- Inspection and Screening Systems

The equipment categories are listed on the web-based AEL on the Responder Knowledge Base (RKB), which is sponsored by DHS and at *https://www.rkb.us/*.

Equipment Standards
Unless otherwise stated in the Grant Guidance, equipment must meet all mandatory regulatory and/or DHS-adopted standards to be eligible for purchase using these funds. Compliance must be demonstrated either via third-party certification by an approved certifying organization or, where permitted by the standard, a supplier's declaration of conformity (SDOC) with appropriate supporting data and documentation per ISO/IEC 17050. In addition, agencies will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment.

A list of mandatory standards for each equipment item can be found at the following website*: https://www.rkb.us/*

2. Training. Nonprofit organization security personnel may use NSGP funds to attend security-related training courses and programs. Allowable training-related costs under NSGP are limited to attendance fees for the training, and related expenses, such as materials, supplies, and/or equipment. Overtime, backfill, and/or travel expenses are not allowable costs. Allowable training topics are limited to the protection of CIKR,

including physical and cyber security, target hardening, and terrorism awareness/employee preparedness.

Training conducted using NSGP funds must address a specific threat and/or vulnerability, as identified in the nonprofit's Investment Justification. ***Proposed attendance at training courses and all associated costs leveraging the FY 2008 NSGP must be included in the nonprofit organization's Investment Justification***.

Nonprofit organizations are required, within 30 days after attendance, to submit information to the SAA on all training supported with NSGP funds. This information will consist of course title, course description, mission area, level of training, the training provider, the date of the course, and the number and position titles of the individuals.

Allowable Training Costs
Allowable training-related costs include the following:

- **Funds used to attend training,** including costs related to attendance of the training, and related expenses, such as materials, supplies, and/or equipment.

3. Management and Administrative (M&A). No more than three percent (3%) of the total award amount may be used for M&A purposes. M&A activities are those defined as directly relating to the management and administration of the grant funds, such as financial management and monitoring.

M&A costs include the following categories of activities:

- Hiring of full-time or part-time staff or contractors/consultants:
  - To assist with the management of UASI NSGP funds
  - To assist with design, requirements, and implementation of the UASI NSGP
  - Meeting compliance with reporting/data collection requirements, including data calls
- Development of operating plans for information collection and processing necessary to respond to DHS data calls
- Travel expenses directly related to management and administration of UASI NSGP funds
- Meeting-related expenses directly related to management and administration of UASI NSGP funds

APPENDIX A.
INVESTMENT JUSTIFICATION

Applicants will be required to submit Investment Justifications for funding requests that addresses the threat-oriented eligibility criteria as well as specific information on what activities will be implemented, what outcomes will be achieved, how the investment will be managed, and how the investment and related security enhancement activities are being coordinated with relevant state and local authorities.

In five pages or fewer using 12 point Times New Roman font and double-spaced lines, applicants must:

- Describe their nonprofit organization, including:
    - Membership and community served
    - Symbolic value of the site(s) as a highly recognized national or historical institution that renders the site a possible target of international terrorism
    - Known critical infrastructure or key resources (CIKR) located within close proximity to nonprofit organization facilities (see *http://www.dhs.gov/nipp* for additional information and guidance on CIKR sectors)
    - Any role in responding to or recovering from international terrorist attacks
- Identify prior threats or attacks (within or outside the U.S.) by a terrorist organization, network, or cell against their nonprofit organization or a closely related organization. Explain how their nonprofit organization gained knowledge of these threats, including the source of the information, and how this understanding influenced development of this application.
- Describe findings from previously conducted risk assessment, including threat and vulnerability.
- Describe the proposed target hardening activity, including total funds requested, that addresses the identified threat and vulnerability.
- Describe the project management, including:
    - Who will manage the project
    - Milestones, with start and end dates
    - Description of any challenges to the effective implementation of this project
    - Coordination of the project with state and local homeland security partners
    - Anticipated outcomes achieved.
- Describe how the 75-25 soft match will be met (see Section III of the guidance).
- Identify whether their nonprofit organization has previously received any homeland security preparedness funding through their State and/or Urban Area, including the DHS Homeland Security Grant Program (including Urban Areas Security Initiative, UASI NSGP, State Homeland Security Program, and/or Citizen Corps Program).

APPENDIX B.
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 the NSGP. 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 24 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 4th 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.

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.

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 though 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 NSGP 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.

7. State Preparedness Report. Congress requires that States receiving DHS-administered Federal preparedness assistance shall submit a State Preparedness

Report to the Department on the State's level of preparedness by March 31, 2008, and annually thereafter. The report shall include: (1) an assessment of State compliance with the national preparedness system, NIMS, the NRP, and other related plans and strategies; (2) an assessment of current capability levels and a description of target capability levels; and (3) an assessment of resource needs to meet the National Preparedness Priorities, including an estimate of the amount of expenditures required to attain the Priorities and the extent to which the use of Federal assistance during the preceding fiscal year achieved the Priorities.

E. Monitoring

Grant recipients will be monitored periodically by 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 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*. Eligible SAAs must apply for funding through this portal, accessible on the Internet at *http://www.grants.gov*.

Application attachments submitted via *grants.gov* must be in one of the following formats: Microsoft Word (*.doc), PDF (*.pdf), or text (*.txt). Use the Catalog of Federal Domestic Assistance (CFDA) number listed in the relevant program guidance section of this document in *grants.gov*.

This Appendix is intended to provide guidance on the various steps and activities associated with filing an application using *grants.gov.*

Step 1: Registering.

Registering with *grants.gov* is a one-time process; however, if you are a first time registrant **it could take 3-5 business days to have your registration validated, confirmed, and receive your user name and password**. It is highly recommended you start the registration process as early as possible to prevent delays in submitting your application package to our agency by the deadline specified. While your registration is pending, you may continue with steps 2, 3, and 4 of these instructions. Registration must be complete for you to be able to submit (step 5) and track (step 6) an application.

1. Establishing an e-business point of contact. *grants.gov* requires an organization to first be registered in the CCR before beginning the *grants.gov* registration process. If you plan to authorize representatives of your organization to submit grant applications through *grants.gov*, proceed with the following steps. If you plan to submit a grant application yourself and sign grant applications and provide the required certifications and/or assurances necessary to fulfill the requirements of the application process, proceed to DUNS Number and then skip to the Authorized Organization Representative and Individuals section.

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

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

- To begin the registration process, click the "Register your Organization [Required]" or "Complete Registration Process [Required]" links. You may print a

registration checklist by accessing
www.grants.gov/assets/OrganizationRegCheck.pdf.

2. DUNS number. You must first request a Data Universal Numbering System number. Click "Step 1. Request a DUNS Number." If you are applying as an individual, please skip to "Authorized Organization Representative and Individuals." If you are applying on behalf of an organization that already has a DUNS number, please proceed to "Step 2. Register with Central Contractor Registry (CCR)." You may obtain a DUNS number at no cost by calling the dedicated toll-free DUNS number request line at 1–866–705–5711.

3. Central Contractor Registry. Registering with the CCR, updating or changing your profile could take up to three to five business days to be confirmed and validated. This delay could prevent your application from being submitted by the deadline specified, so you should register or make changes to your profile as early in the process as possible.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

registration process, *grants.gov* will notify the <u>e-Business POC</u> for assignment of user privileges.

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

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

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

Step 2: **Downloading the Application Viewer.**

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

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

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

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

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

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

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

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

- Click "Next" to continue.

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

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

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

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

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

Step 3: **Downloading an Application Package.**

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

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

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

- Enter the CFDA number for this announcement, **97.078**. Then click "Download Package." This will take you to the "Selected Grants Application for Download" results page.

- To download an application package and its instructions, click the corresponding download link below the "Instructions and Application" column.

- Once you select a grant application, you will be taken to a "Download Opportunity Instructions and Application" screen to confirm that you are downloading the correct application. If you would like to be notified of any changes to this funding opportunity, enter your e-mail address in the corresponding field, then click the "Submit" button.

- After verifying that you have downloaded the correct opportunity information, click the "Download Application Instructions" button. This will open a PDF of this grant solicitation. You may print the solicitation or save it to your computer by clicking either the print icon at the top tool bar or the "File" button on the top tool bar. If you choose to save the file, click on "Save As" and save to the location of your choice.

- Click the "Back" Navigation button to return to the "Download Opportunity Instructions and Application" page. Click the "Download Application Package" button. The application package will open in the PureEdge Viewer.

- Click the "Save" button to save the package on your computer. Because the form is not yet complete, you will see a prompt that one or more fields may be invalid. You will complete these fields in step 4, but for now, select "Yes" to continue. After you click "Yes," the "Save Form" window will open.

- Save the application package to your desktop until after submission. Select a name and enter it in the "Application Filing Name" field. Once you have submitted the application through *grants.gov*, you may then move your completed application package to the file location of your choice.

- Click the "Save" button. If you choose, you may now close your Internet browser and complete your application package offline by double clicking the icon on your desktop. You do not have to be connected to the Internet to complete the application package in step 4 below.

Step 4: Completing the Application Package.

This application can be completed entirely offline; however, you will need to log in to *grants.gov* to submit the application in step 5.

- Locate the application package you saved on your computer. When you open the package, it will be in PureEdge Viewer. You may save your application at any time by clicking on the "Save" button at the top of the screen.

- Enter a name for your application package in the "Application Filing Name" field. This can be a name of your choice.

- Open and complete all the mandatory and optional forms or documents. To complete a form, click to select the form, and then click the "Open" button. When you open a required form, the mandatory fields will be highlighted in yellow. If you enter incomplete information in a mandatory field, you will receive an error message or the field will turn red, indicating a change needs to be made.

- Mandatory forms include the: (1) Application for Federal Assistance (SF-424); (2) Assurances for Non-Construction Programs (SF-424B); and (3) Disclosure of Lobbying Activities (SF-LLL). These forms can also be viewed at *http://apply.grants.gov/agency/FormLinks?family=7*.   Other mandatory forms are identified in Section IV.

- When you have completed a form or document, click the "Close Form" button at the top of the page. Your information will automatically be saved.

- Next, click to select the document in the left box entitled "Mandatory Documents." Click the "=>" button to move the form or document to the "Mandatory Completed Documents for Submission" box to the right.

- Some mandatory documents will require you to upload files from your computer. To attach a document, select the corresponding form and click "Open." Click the "Add Mandatory Attachment" button to the left. The "Attach File" box will open. Browse your computer to find where your file is located and click "Open." The name of that file will appear in the yellow field. Once this is complete, if you would like to attach additional files, click on the "Add Optional Attachment" button below the "Add Mandatory Attachment" button.

- An "Attachments" window will open. Click the "Attach" button. Locate the file on your computer that you would like to attach and click the "Open" button. You will return to the "Attach" window. Continue this process until you have attached all the necessary documents. You may attach as many documents as necessary.

- Once you have finished, click the "Done" button. The box next to the "Attach at Least One Optional Other Attachment" will now appear as checked.

- *Note:* the name of these buttons will vary depending on the name of the form you have opened at that time; i.e., Budget Narrative, Other Attachment, and Project Narrative File.

- To exit a form, click the "Close" button. Your information will automatically be saved.

Step 5: **Submitting the Application.**

Once you have completed all the yellow fields on all the forms and saved the application on your desktop, check the application package for errors. This can be done any time throughout step 4 above and as often as you like.

- When you are ready to submit your final application package, the "Submit" button at the top of your screen will be enabled. This button will not be activated unless all mandatory data fields have been completed. When you are ready to submit your application, click on "Submit." This will take you to a "Summary" screen.

- If your "Submit" button is not activated, then click the "Check Package for Errors" button at the top of the "Grant Application Package" screen. PureEdge Viewer will start with the first form and scan all the yellow fields to make sure they are complete. The program will prompt you to fix one error at a time as it goes through the scan. Once there are no more errors, the system will allow you to submit your application to *grants.gov.*

- Review the application summary. If you wish to make changes at this time, click "Exit Application" to return to the application package, where you can make changes to the forms. To submit the application, click the "Sign and Submit Application" button.

- This will take you to a "Login" screen where you will need to enter the user name and password that you used to register with *grants.gov* in "Step 1: Registering." Enter your user name and password in the corresponding fields and click "Login."

- Once authentication is complete, your application will be submitted. Print this confirmation screen for your records. You will receive an e-mail message to confirm that the application has been successfully uploaded into *grants.gov*. The confirmation e-mail will give you a *grants.gov* tracking number, which you will need to track the status of your application. The confirmation e-mail will go to the e-Business POC; therefore, if you are submitting on behalf of someone else, be sure the e-Business POC is aware of the submission and that a confirmation e-mail will be sent.

- When finished, click the "Close" button.

Step 6: **Tracking the Application.**

After your application is submitted, you may track its status through *grants.gov*. To do this, go to the *grants.gov* home page at *http://www.grants.gov*. At the very top of the screen, click on the "Applicants" link. Scroll down the "For Applicants" page and click the

"Login Here" button. Proceed to login with your user name and password that was used to submit your application package. Click the "Check Application Status" link to the top left of the screen. A list of all the applications you have submitted through *grants.gov* is produced. There four status messages your application can receive in the system:

- **Validated.** This means your application has been scanned for errors. If no errors were found, it validates that your application has successfully been submitted to *grants.gov* and is ready for the agency to download your application.

- **Received by Agency.** This means our agency DHS downloaded your application into our electronic Grants Management System (GMS) and your application is going through our validation process to be successfully received on our end.

- **Agency Tracking Number Assigned.** This means our GMS did not find any errors with your package and successfully downloaded your application into our system.

- **Rejected With Errors.** This means your application was either rejected by *grants.gov* or GMS due to errors. You will receive an e-mail from *grants.gov* customer support, providing details of the results and the next steps required. Most applications are rejected because: (1) a virus was detected; (2) you are using a user name and password that has not yet been authorized by the organization's e-Business POC; or (3) the DUNS number you entered on the SF-424 form does not match the DUNS number that was registered in the CCR for this organization.

If you experience difficulties at any point during this process, please call the *grants.gov* customer support hotline at 1–800–518–4726.

APPENDIX D.
ADDITIONAL RESOURCES

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

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.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* to find the point of contact in your area. For assistance at the national level, contact Tricia Reed *at* 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/government/grant/index.shtm*.

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 NSGP 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 or (202) 324-8833. For additional information on HSIN and available technical assistance, contact the HSIN Help Desk at (703) 674-3003.