U.S. Department of Homeland Security
Office of Grants and Training

FY 2006 Infrastructure Protection Grant Program: *Buffer Zone Protection*

Program Guidelines and Application Kit

Foreword

I am pleased to provide you the Fiscal Year (FY) 2006 program guidelines and application materials for grants under the U.S Department of Homeland Security (DHS) Infrastructure Protection Grant Program Buffer Zone Protection.

This is the first grant cycle since completion of the Department's Second Stage Review last summer and our creation of a unified Preparedness Directorate. The preparedness mission transcends the entire Department. Our approach to preparedness aggregates critical assets within DHS to support our operating components and the work of our external partners to prevent, protect against, deter, respond to, and recover from terrorist attacks, and to continuously mitigate threats to America's safety and security. The Preparedness Directorate performs the strategic function of integrating people, funding and programs.

The new Preparedness Directorate includes the essential work of the Department's Office of Grants and Training (G&T). In managing our grant programs, DHS is committed to supporting risk-based investments. We are equally committed to continuous innovation. As new infrastructure is built, existing facilities improved, or as our assessment of specific threats change, DHS grant programs will focus on being nimble and making high-return investments to combat terrorism.

In 2006, $373 million is available for a package of inter-related infrastructure protection grants. The FY 2006 Buffer Zone Protection Program makes up to $48 million available. These grants are a vital tool in making our nation safer in the war on terror. They provide assistance for physical security enhancements to some of the Nation's most at-risk critical infrastructure.

For each grant, the Preparedness Directorate will rely on an integrated team of subject matter experts drawn from DHS operating components to develop, design, compete, review, and support the infrastructure grants as part of the national preparedness effort. Specifically, with respect to buffer zone protection:

- The Office of Infrastructure Protection (IP), a component of the Preparedness Directorate, has the lead for assuring the grants accomplish required objectives, such as continuing to refine the risk-based allocation of funds in 2006. This process will hasten the development of an integrated risk-based decision making process for each region. Specifically, IP will review the programmatic and planning activities and requested equipment to ensure that they achieve a reasonable risk reduction. This risk reduction should be achieved through reducing the likelihood that adversaries would succeed in attacks through increased protection in the buffer zone and may be augmented by plans that reduce the potential consequences or otherwise deter attacks.

- G&T provides design, facilitation, administration, coordination and financial management of these programs, as well as the integration of these programs with national preparedness efforts, including the National Preparedness Goal. G&T also coordinates with other relevant parts of the DHS family to bring their subject matter expertise to bear on specific grants and initiatives.

DHS is committed to working with the owners and operators of America's critical infrastructure as part of the national effort to reduce the risks from terrorism and other threats to the homeland.

Michael Chertoff
Secretary
Department of Homeland Security

Contents

I. Introduction 1

II. The FY 2006 Buffer Zone Protection Program 2

III. Eligible Applicants and Funding Availability 7

IV. Program and Application Requirements 12

V. Assistance, Resources and Support 26

VI. Reporting, Monitoring and Closeout Requirements 28

Appendix A Authorized Program Expenditures Guidance A-1

Appendix B Historical Allowable Data B-1

Appendix C Relationship of BZPP Grant Programs to Target Capabilities C-1

Appendix D Grants.gov Quick-Start Instructions D-1

Appendix E Post Award Instructions E-1

Appendix F Additional Guidance on the National Preparedness Goal and the National Priorities F-1

Appendix G Capabilities Based Planning Guidance G-1

Appendix H National Incident Management System Guidance H-1

Appendix I National Infrastructure Protection Plan I-1

Appendix J Domestic Nuclear Detection Office Guidance J-1

Appendix K Acronyms and Abbreviations K-1

I. Introduction

The FY 2006 Buffer Zone Protection Program (BZPP) is an important component of the Administration's larger, coordinated effort to strengthen the security of America's critical infrastructure. This program implements the objectives addressed in a series of laws, strategy documents, plans and Homeland Security Presidential Directives (HSPDs). Of particular significance are the National Preparedness Goal (the Goal)* and the National Infrastructure Protection Plan (NIPP)*.

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

On March 31, 2005, DHS issued the Interim National Preparedness Goal. The Goal establishes a vision for a National Preparedness System. A number of the key building blocks for that system, including the National Planning Scenarios, Universal Task List (UTL), Target Capabilities List (TCL), and the seven National Priorities are important components of a successful BZPP.

* As this grant guidance went to print, the final Goal and the NIPP were also being prepared for release.

II. The FY 2006 Buffer Zone Protection Program

A. Program Overview

The FY 2006 BZPP, as a component of the Infrastructure Protection Program (IPP), provides funds to build capabilities at the State and local levels to prevent and protect against terrorist incidents. This is primarily done through planning and equipment acquisition. These capabilities support the implementation of the goals included in Homeland Security Strategies, including the NIPP. BZPP funding directly supports the prevention and protection mission areas and addresses many of the National Priorities, as well as the related target capabilities.

The FY 2006 BZPP provides funds to support the implementation of Buffer Zone Plans (BZPs) outside the perimeter of identified critical infrastructure/key resource (CI/KR) sites. These plans are intended to develop effective preventive and protective measures that make it more difficult for terrorists to conduct surveillance or launch attacks within the immediate vicinity of high priority critical infrastructure targets. They also increase the preparedness capabilities of the local jurisdiction(s) responsible for the security and safety of the surrounding communities.

In developing the BZP, the responsible local jurisdiction(s) should review and assess ways in which they can work with relevant Federal, State, local, Tribal, and private sector agencies to coordinate their prevention and protection activities. This coordination will enable all relevant agencies at all levels of government to more effectively carry out their existing programs. BZPs accomplish the following steps:

- Identify significant assets at the site that may be targeted by terrorists for attack;
- Determine specific threats and vulnerabilities associated with the site and its significant assets;
- Develop an appropriate buffer zone extending outward from the facility in which protective measures can be employed to make it more difficult for terrorists to conduct site surveillance or launch attacks;
- Implement preventive and protective measures within a buffer zone that will reduce the risk of a successful terrorist attack by:
    - **Devaluing** a target by making it less attractive or too costly to attack;
    - **Deterring** an event from happening (e.g., through warning signs, physical barriers, cameras, and security guards);
    - **Detecting** an aggressor who is planning or committing an attack or the presence of a hazardous device or weapon; and,
    - **Defending** against attack by delaying or preventing an aggressor's movement toward the asset or use of weapons and explosives.

- Identify all applicable law enforcement jurisdictions at all levels of government with a role in the prevention of, protection against, and response to terrorist threats or attacks specific to the site and appropriate points of contact within these organizations;
- Evaluate the capabilities of the responsible law enforcement jurisdictions with respect to terrorism prevention and response; and,
- Identify specific planning, equipment, training, and exercise capabilities needed by the responsible jurisdictions to mitigate the threats and vulnerabilities of the site and its buffer zone and enhance preparedness capabilities of the surrounding community.

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.

B. BZPP Process Overview

Use of FY 2006 BZPP funds **must** be consistent with the State and/or Urban Area Homeland Security Strategy. Therefore, the BZP and Vulnerability Reduction Purchasing Plan (VRPP) must be coordinated between the State Administrative Agency (SAA) and Homeland Security Advisor (HSA), as well as any applicable State strategy planning teams, Urban Area Working Groups (UAWG), Regional Transit Security Working Groups (RTSWG), and/or Area Maritime Security Committees. This will allow the plans to be synchronized with the development and implementation of State and/or Urban Area Homeland Security Strategies, and all other ongoing prevention, protection, response, and recovery initiatives, programs, and funding sources within the State. Linkages between specific projects undertaken with BZPP funds and strategic goals and objectives will be highlighted in the VRPP and through regular required reporting mechanisms, including the Biannual Strategy Implementation Reports (BSIR). The following steps, outlined in Figure 2, must be completed for each identified site before grant funds for the FY 2006 BZPP may be obligated, drawn down, or expended by the State to the responsible local jurisdiction for the CI/KR site:

Figure 2. BZPP Process Flow

- Responsible local jurisdictions should leverage existing vulnerability and capability assessments, or conduct necessary assessments, if appropriate.
  - Coordinate with security management and measures already in place at the facility.
- Responsible local jurisdictions use DHS-developed templates and processes to develop a BZP and VRPP for identified sites.
- Responsible local jurisdictions **must** coordinate the development of the BZP and VRPP with:
  - The State (SAA and HSA);
  - Urban Area Working Groups (UAWG), if applicable;
  - Urban Area Homeland Security Strategies, if applicable;
  - Regional Transit Security Working Groups (RTSWG), if applicable; and,
  - Area Maritime Security Committees, if applicable.
- Upon completion, the responsible local 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 funding programs; and,
  - Certification that the BZP and equipment requested in the VRPP supports and/or compliments a) Statewide efforts to develop a Critical Infrastructure Protection (CIP) program and CIP 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.
- SAA submits the certified BZP and VRPP to the DHS Preparedness Directorate for review.
- Upon DHS Preparedness Directorate approval, the SAA can drawdown and expend funds to implement the BZP.

C. BZPP Process Requirements

1. Development of the BZP and VRPP

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

2) The responsible local jurisdictions are required to share these assessments with the Preparedness Directorate upon request, so that DHS may better prioritize

preventive and protective programs, as they may be relevant to emerging and specific threats.

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

    - UAWGs
    - RTSWGs
    - Area Maritime Security Committees

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

4) Upon completion of the BZP, the local jurisdiction must complete a VRPP. The VRPP identifies a spending plan, including the planning activities and equipment necessary to implement the BZP.

2. Submission of the BZP and VRPP

1) 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 CIP Program funding.

2) 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:

    a) Statewide efforts to develop a CIP program and associated capabilities, as directed in the NIPP; and,
    b) The implementation of the NIPP national priority, as reflected within each respective State's Homeland Security Strategy.

3) Upon certification, the SAA must submit the BZP and VRPP for each site to DHS for review and approval by February 1, 2007.

4) The BZPs and VRPPs must be submitted electronically via *the G&T Secure Portal* located at https://odp.esportals.com/. The *G&T Secure Portal* will contain a FY 2006 BZPP folder for each State.

5) The certified BZPs and VRPPs will be reviewed by the DHS Preparedness Directorate to ensure that BZPP programmatic and planning activities and

requested equipment are coordinated with overall Statewide CIP efforts, and related strategic goals and objectives.

6) Upon review and approval of the BZPs and VRPPs by the DHS Preparedness Directorate, the SAA will be notified via email and the responsible local jurisdiction(s) may drawdown and expend grant funds obligated by the SAA for implementation of the BZP. *Note: If the BZP and/or VRPP are incomplete or do not meet program requirements, the SAA may be requested to re-submit program materials or provide additional information*.

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

DHS must receive completed BZPs and VRPPs for all CI/KR sites receiving funding through the FY 2006 BZPP from the SAA by February 1, 2007. If States fail to submit all BZPP materials by this date, funds may be deobligated by G&T.

Funds under the FY 2006 BZPP may not be obligated, drawn down, or expended by the State to the responsible local jurisdiction of the identified site until all of the above steps have been completed by the jurisdiction and approved by DHS.

III. Eligible Applicants and Funding Availability

A. Eligible Applicants

The Governor of each State has designated a SAA to apply for and administer the funds under BZPP.[1] The SAA is the only agency eligible to apply for BZPP funds and is responsible for obligating BZPP funds to the appropriate local units of government or other designated recipients.[2] The SAA must coordinate all BZPP activities with the respective State HSA.

B. Approach to FY 2006 BZPP Site Selection

The FY 2006 BZPP site selection process is built upon the DHS risk methodology. Identifying the risks to the nation's critical infrastructure is an important component of the Department's overall risk reduction programs. The FY 2006 iteration of the methodology represents a major step forward in the analysis of the risk of terrorism faced by our Nation's communities. Tremendous gains have been made in both the quality and specificity of information and analysis incorporated within the model, yielding the most accurate estimation possible of the *relative* risk of prospective grantees.

1. In accordance with the Department's emphasis on prioritizing programmatic activities based upon objective measures of risk, CI/KR sites in the National Asset Database (NADB) have been selected for participation in the FY 2006 BZPP using a risk-based analytic approach. The Department, working with its partners in each State and representatives of the 17 CI/KR sectors, has identified those sites in the United States that represent the most at risk critical infrastructures based on an analysis of consequence, and available vulnerability and threat data.

2. Using asset-based risk to guide the allocation of fund to specific sites within the United States. This approach generates risk reduction benefits for the greater community as well as at each site.

3. Determining state allocation based on the number of higher-risk sites;

[1] 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."

[2] As defined in the Conference Report accompanying the Department of Homeland Security Appropriations Act of 2006, the team "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."

Site-Specific Analysis

DHS worked with SSAs, States, and the private sector to identify the top 100 sites for each sector and evaluated them to determine which could have significant effect if lost or disrupted, as well as those sites that could have a regional or cross-jurisdictional impact if lost or disrupted. DHS then conducted vulnerability and threat analysis to evaluate how likely an attacker would be to succeed in attacking these assets and how likely an attacker would be to attempt it. Based on the results of this analysis, DHS identified the list of the select high-risk sites for consideration in the FY 2006 BZPP by analyzing the following:

- Consequence: The Department's risk analysis office at Oak Ridge National Laboratory performed asset-based consequence analysis on each asset identified for eligibility. Factors used in this analysis include potential impacts on public health and safety, the economy, national morale, and delivery of national essential functions.
- Vulnerability: The likelihood that an attacker would succeed in exploiting a weakness to gain access or cause damage to a given asset type. Vulnerability data is derived from subject matter experts, DHS analysis of the vulnerability of asset classes, and vulnerability assessments at specific sites.
- Threat: DHS capability to assess threats by infrastructure sector has greatly improved over the last fiscal year. The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), the Department's infrastructure-intelligence fusion center, provided measures of the likelihood that a specific type of attack will be initiated against a specific target type. HITRAC coordinates this effort with the Intelligence Community (IC) to ensure that all credible threats and incidents collected by the IC, operational indicators of terrorist activity, and assumptions of terrorist capability and intent are included in DHS analysis for the FY2006 BZPP.

Risk Analysis

In addition to site-specific risk analysis, an important component of the Buffer Zone process is its ancillary benefits to the surrounding community. Identification of high-risk jurisdictions helps ensure that the Buffer Zone Protection Program will reduce risk to a broader array of at-risk assets, as well as enhance the preparedness of State and local governments.

The Department's methodology to determine high-risk jurisdictions brings together two separate, but complementary, types of risk: ***asset-based risk*** and ***geographically-based risk***. Considered together, these two calculations provide an estimate of total terrorism risk to a given region, evaluating both risks to assets within a State or territory, as well as risk related to the unique characteristics of the candidate States, territories, and the District of Columbia.

Asset-based risk is a function of the risk of terrorism to potential targets within a geographic area. It accounts for the combined risks associated with the various assets within the "footprint" of each individual candidate. Asset-based risk allows DHS to

strategically evaluate the likelihood of terrorist attacks against assets based on input from Intelligence Community assessments, the likelihood that such attacks would succeed, and the consequences of these attacks, based upon the work of subject matter experts, sector-specific agencies (SSAs), and the growing knowledgebase in the DHS NADB. Asset-based risk analysis considered 40 different asset types.

Geographically-based risk is derived from certain prevailing attributes or characteristics intrinsic to each geographical area that may contribute to its risk of terrorism. This approach incorporates types of threat data that are independent of a specific, identifiable asset, such as reports on possible threatening activities within a given geographic area. Similarly, through this approach, DHS has considered variables such as population or other general characteristics that are not linked to one particular type of asset. This approach considers characteristics of the area that give it inherently more risk, such as:

- The number of current terrorism investigations,
- A review of intelligence and suspicious activity reporting,
- The presence of international borders,
- The number of visitors through international ports of entry,
- The size and density of its population,
- The value of its agricultural products,
- The number of national defense assets within the state, and
- A variety of other CI/KR related risk-based factors

C. Funding Availability

Based upon the results of this analysis, 53 States, Territories, and the District of Columbia are eligible to participate in and receive funding under the FY 2006 BZPP. These States and the funding allocated to each State are identified in Table 1. The specific sites and their locations are sensitive; however, DHS will provide each State with information regarding the identity and location of specific high-risk sites in their respective State.

The FY 2006 BZPP funding will support activities at two categories of critical sites described below:

1. Candidate sites within the State that are <u>eligible</u> for funding under the FY 2006 BZPP, based on the results of the risk analysis. States will have an opportunity to select which of the candidate sites will receive funding under the FY 2006 BZPP, in collaboration with DHS and the SSAs. In this process States are encouraged to evaluate and select sites that support the development and implementation of regional and/or cross-jurisdictional prevention and protection capabilities.

2. A select subset of high-risk sites nationwide that are <u>mandated</u> for inclusion by appropriate States in the FY 2006 BZPP based on the results of the risk analysis.

Due to increased funding and eligible program costs, sites and their respective jurisdictions that participated in the FY 2005 BZPP may be included on the list of sites eligible for funding in FY 2006. Likewise, sites selected for funding under the FY 2006 BZPP may also be eligible for funding under future DHS Infrastructure Protection Programs.

Table 1. FY 2006 BZPP Funding Allocations

States / Territories	Total Funding
Alabama	$378,000
Alaska	$1,189,000
Arizona	$567,000
Arkansas	$378,000
California	$5,835,000
Colorado	$189,000
Connecticut	$189,000
Delaware	$189,000
District of Columbia	$567,000
Florida	$1,701,000
Georgia	$567,000
Hawaii	$189,000
Idaho	$189,000
Illinois	$2,079,000
Indiana	$567,000
Iowa	$189,000
Kansas	$378,000
Kentucky	$567,000
Louisiana	$2,268,000
Maine	$189,000
Maryland	$756,000
Massachusetts	$2,134,000
Michigan	$1,945,000
Minnesota	$567,000
Mississippi	$189,000
Missouri	$756,000
Montana	$189,000
Nebraska	$189,000
Nevada	$1,189,000
New Hampshire	$189,000
New Jersey	$1,512,000
New Mexico	$189,000
New York	$6,591,000
North Carolina	$378,000

North Dakota	$500,000
Ohio	$1,323,000
Oklahoma	$189,000
Oregon	$189,000
Pennsylvania	$1,756,000
Puerto Rico	$189,000
Rhode island	$189,000
South Carolina	$756,000
South Dakota	$500,000
Tennessee	$945,000
Texas	$2,268,000
Utah	$378,000
Vermont	$189,000
Virginia	$945,000
Virgin Islands	$189,000
Washington	$1,756,000
West Virginia	$189,000
Wisconsin	$189,000
Wyoming	$189,000
Total	**$47,965,000**

IV. Program and Application Requirements

A. General Program Requirements

The following section highlights important guidance, policy, and coordination requirements applicable to the FY 2006 BZPP. Applicants should pay close attention to the language in this section, as this year's guidance has been adjusted to reflect the new strategic context of the Goal and the National Priorities, and how they relate to Targeted Infrastructure Protection Programs (TIPP).

State and Urban Area Homeland Security Strategies were recently updated to reflect the Goal, and will continue to serve as the overarching guide for homeland security efforts as the Goal is finalized. These strategy updates represent an important first step in transitioning to the common framework for building, sustaining, and improving national preparedness for a broad range of threats and hazards that is envisioned in the Goal. While developing the application for the FY 2006 BZPP, grantees are encouraged to look across all available support and assistance programs and leverage all available funding and resources from multiple sources, wherever possible, to effectively implement the NIPP.

1. Period of Performance. The period of performance for the FY 2006 BZPP is **24 months** from the date of award. Any unobligated funds will be deobligated by G&T at the end of this period. Extensions to the period of performance will be considered only through formal requests to G&T with specific and compelling justifications as to why an extension is warranted.

2. Pass-Through Requirements. Each State shall make no less than **95 percent** of the total grant program amount available to local units of government within 60 days of the approval notification for the VRPP.

3. Memorandum of Understanding (MOU) Requirements. The State may retain some or all of the local unit of government allocation of grant funds under the FY 2006 BZPP for expenditures made by the State on behalf of the local unit of government or Urban Area. This may occur only if requested in writing by that local unit of government or Urban Area. States holding grant funds on behalf of local units of government or Urban Areas must enter into a formal MOU with the local unit of government or Urban Area specifying the amount of funds to be retained by the State and the intended use of funds.

If an MOU is already in place from FY 2005, G&T will continue to recognize the MOU for FY 2006. If any modifications to the existing MOU are necessary to reflect new initiatives, States should contact their assigned Preparedness Officer.

Any new MOU request must be initiated by the local unit of government or Urban Area. The following elements must be included in the creation of an MOU. Alternatively,

States may contact their G&T Preparedness Officer to obtain a template for preparing the document, and may elect to submit it to him or her for review.

- Parties to the agreement
- Authority to enter into the agreement
- Purpose of the agreement
- Responsibilities of each party in the agreement
- Points of Contact for each party to the agreement
- Any other provisions or terms of the agreement
- Effective dates
- Modification clause
- Termination clause
- Approval signatories

A final, executable copy of the MOU will be kept on file with the SAA and be made available to DHS upon request.

4. Integrating Preparedness Assistance. The Goal established a common planning framework in which agencies at all levels of government and across all disciplines can operate. This new strategic framework provides the Nation with an opportunity to begin viewing programs that have traditionally been managed within one particular agency or discipline in a more holistic and connected manner. Only when programs are managed and implemented through an interdisciplinary and multi-jurisdictional approach can the Nation truly begin to operate in the coordinated fashion that a major disaster or catastrophic event will demand.

Using the Goal and the corresponding structure of the TCL as a foundation, State and local homeland security, public safety, and public and private health organizations can continue to build the framework that connects them to support the overall homeland security program. Appendix C maps the BZPP, along with the HSGP and other DHS preparedness programs, to each of the Target Capabilities in an effort to emphasize areas of overlap among the programs as well as any unique focus areas of each program.

States should examine how they are integrating preparedness activities across disciplines and agencies. As part of the FY 2006 HSGP planning process, States must implement a cohesive planning framework that builds and implements homeland security initiatives that leverage DHS resources, as well as other Federal and State resources. In addition to DHS support, grantees and subgrantees should consider preparedness assistance programs from other Federal SSAs including the U.S. Department of Agriculture (USDA), Department of Justice (DOJ), and Department of Transportation (DOT). Specific attention should be paid to how all available preparedness funding sources can be effectively utilized in a collaborative manner to support the enhancement of capabilities throughout the State and/or local jurisdictions. This underscores the importance that DHS and SSAs stress to grantees and subgrantees in taking a holistic approach to implementing their strategic homeland

security goals and objectives by considering all available support and assistance programs, regardless of the source.

5. Effective State Homeland Security Programs. An effective homeland security program hinges on sound program governance structures that help ensure the program is capable of conducting business across Departments, agencies, and disciplines at all levels of government. Because such a wide spectrum of stakeholders are involved in efforts to prevent, protect against, deter, respond to, recover from, and mitigate major events, governance can present unique challenges. Although a lead State agency is required from a functional standpoint to manage the overall homeland security program, the scope of the program transcends agencies and demands collaboration among all key constituencies in order to achieve success.

The State homeland security program should provide a strategic management framework to ensure consistency among the full range of program-related activities and operational plans and procedures. The State homeland security program should also work to achieve and sustain risk-based target levels of capability to prevent, protect against, respond to, and recover from catastrophic events and acts of terrorism in order to minimize the impact on lives, property, and the economy. This includes achieving the target capabilities necessary to protect CI/KR deemed critical at the National, State, and local level.

6. State and Urban Area Homeland Security Strategies. For FY 2006, State and Urban Area Homeland Security Strategies will continue to provide the overarching strategic vision for the implementation of State and Urban Area homeland security programs, which include State and Urban Area CIP programs. States and Urban Areas were recently required to update their strategies to bring the strategies into alignment with the National Priorities included in the Goal. Updated State and Urban Area Homeland Security Strategies continue to provide the context for the evaluation of preparedness programs and capabilities within and across State boundaries.

7. Coordination Requirements

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

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

ensure all programs, plans, and requested resources are coordinated and leveraged across the region.

- ***Transit and Port Security Coordination***
  In the development of the FY 2005 Regional Transit Security Strategies (RTSS), mass transit systems were aligned to their respective State and Urban Area Homeland Security Strategies in order to establish a regional, collaborative vision for transportation security. This regional collaboration effort was augmented under the FY 2005 Transit Security Grant Program (TSGP) with the establishment of the RTSWG structure. The RTSWG provides an arena where State, local, tribal, and parish leadership join with respective transit leadership for that region to coordinate a collective approach to managing the needs of the eligible transit grant recipients.

  In many cases, the RTSWG becomes a formal or, at a minimum, an ad-hoc component of the existing UAWGs and/or historical transportation planning organizations (i.e., Metropolitan Planning Organizations) which have responsibility over transit issues. Within the port security arena, the FY 2006 Port Security Grant Program (PSGP) encouraged increased visibility of the Area Maritime Security Committees within Urban Areas in order to enhance their input into regional needs assessment and planning for port security grants.

  State and local jurisdictions are strongly encouraged to consult the RTSWG and the Area Maritime Security Committees, as appropriate, as they are integral to the achievement of regional collaboration for transportation security and a vital component to the development of an overall State CIP program. Please refer to the *FY 2006 Infrastructure Protection Program: Transit Security* for additional information on the RTSWGs and their member organizations. For more information on maritime security issues, refer to the *National Strategy for Maritime Security* which was released on September 20, 2005, and is available at http://www.whitehouse.gov/homeland/maritime-security.html. The *National Strategy for Transportation Security*, which will provide a national, in-depth transportation security approach, is expected to be released within the year.

B. Specific Program Requirements

1. Protected Critical Infrastructure Information (PCII). The security and protection of the nation's critical infrastructures are of paramount importance, not only to the Federal, State and local governments, but also to private utilities, businesses, and industries. The PCII Program, established pursuant to the Critical Infrastructure Information Act of 2002 (CII Act), created a new framework, which enables members of the private sector to voluntarily submit sensitive information regarding the nation's critical infrastructure to DHS with the assurance that the information, if it satisfies the requirements of the CII Act, will be protected from public disclosure. The PCII Program seeks to facilitate greater sharing of critical infrastructure information among the owners and operators of the critical infrastructures and government entities with infrastructure protection

responsibilities, thereby reducing the nation's vulnerability to terrorism. There are benefits for private sector participants in the PCII Program. Primarily, information sharing will result in better identification of risks and vulnerabilities, which will help industry partner with others in protecting key assets.

PCII Program safeguards ensure that all information submitted to the PCII Program Office is properly protected throughout its lifecycle. These safeguards ensure submitted information is:

- Accessed only by authorized individuals
- Used appropriately for analysis of threats and vulnerabilities
- Disseminated only to authorized and properly trained staff
- Protected from disclosure under the Freedom of Information Act and similar State and local laws

For additional information about PCII please contact the DHS PCII Program Office at pcii-info@dhs.gov.

2. Drawdown of Funds. Grantees and subgrantees may elect to drawdown funds up to 120 days prior to expenditure/disbursement. However, DHS/G&T strongly encourages recipients to drawdown funds as close to expenditure as possible to avoid accruing interest. Funds received by both grantees and subgrantees must be placed in an interest-bearing account and are subject to the rules outlined in the Uniform Rule 6 CFR part 9, *New Restrictions on Lobbying*, and the Uniform Rule 28 CFR Part 70, *Uniform Administrative Requirements for Grants and Agreements (Including Subawards) with Institutions of Higher Education, Hospitals and other Non-profit Organizations*, at http://www.gpoaccess.gov/cfr/index.html.

These guidelines state that subgrantees 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 subgrantee may keep interest amounts up to $100 per year for administrative expenses for all Federal grants combined. Please consult the DHS/G&T Office of Grant Operations Financial Guide and applicable OMB Circulars for additional guidance. Although advance drawdown requests may be made, State grantees remain subject to the interest requirements of the Cash Management Improvement Act (CMIA) and its implementing regulations at 31 C.F.R. Part 205. Interest under CMIA will accrue from the time Federal funds are credited to a State account until the time the State pays out the funds or transfers the funds to a subgrantee.

3. Information Technology

- ***National Information Exchange Model***
  DHS, the DOJ, and their associated domains released the National Information Exchange Model (NIEM 0.1) in October 2005. The NIEM 0.1 establishes a single standard Extensible Markup Language (XML) foundation for exchanging information between DHS, DOJ, and supporting domains, such as Justice, Emergency Management, and Intelligence. The base technology for the NIEM is the Global JXDM. The NIEM will leverage both the extensive Global JXDM reference model and the comprehensive Global JXDM XML-based framework and support infrastructure. The intended uses of this initial release are:
    - To introduce NIEM to the broad NIEM stakeholder community within government and industry.
    - To provide the NIEM model and schemas as a base for creating exchange messages for the initial pilot projects that will validate and augment the standard.
    - To allow information technology and standards experts and users to provide feedback on the standard.
    - To begin to identify additional Universal, Common, and Domain-Specific components that could be added to future versions of the standard.

  To support homeland security, public safety, and justice information sharing, DHS requires all grantees to use the latest NIEM specifications and guidelines as follows regarding the use of XML for all BZPP awards:

    - Use NIEM 1.0 or later for information sharing in production systems. The projected released date for NIEM 1.0 is June 30, 2006.
    - Until the release of NIEM 1.0, the latest NIEM specifications and guidance should be used only for the pilots and prototype systems.

  Grantees shall make available without restriction all schemas (extensions, constraint, proxy) generated as a result of this grant, as specified in the guidelines. Further information about the required use of NIEM specifications and guidelines is available at http://www.niem.gov. If there is any question or comment about the use of NIEM specifications and guidelines, please submit it to http://www.niem.gov/contactus.php.

- ***Homeland Security Information Network (HSIN)***
  HSIN is DHS' primary nationwide information sharing and collaboration network, providing secure, encrypted information exchange over the Internet. HSIN web-based portals provide real-time connectivity and interoperability between the National Operations Center (NOC) and Federal, State, regional, local, and Tribal organizations nationwide. The NOC is the primary national-level hub for domestic situational awareness and information fusion and sharing as they relate to the prevention of terrorist attacks and the management of domestic incidents of national significance.

HSIN is composed of multiple, non-hierarchal Communities of Interest (COIs) that offer security partners the means to communicate and share information and to post and retrieve important documents, based on secure access. The specific COIs that have relevance to BZPP are the Critical Infrastructure Warning Network (CWIN) and the Critical Sector (CS). Figure 2 below provides a brief description of the currently available HSIN COIs.

DHS is requiring all State, regional, local, and Tribal entities using FY 2006 BZPP funding in support of information sharing and intelligence fusion and analysis centers to use the HSIN web-based system as the backbone for communication and collaboration with their member agencies and the NOC. The use of the HSIN system will enable participants in these information sharing and intelligence fusion and analysis centers to access intelligence data from multiple systems, irrespective of their own platform or programming language. Participants are also encouraged to use HSIN to conduct data queries and to exchange information and reports with the NOC on a regular basis, in accordance with appropriate State and/or local reporting procedures.

In support of the implementation, integration, and use of HSIN, DHS will offer technical assistance and training in FY 2006 for State and local jurisdictions to adopt, connect to, use, and enhance their familiarity and proficiency with HSIN. This technical assistance will include training and workshops for States and local jurisdictions and member agencies in the use of HSIN and support to certify and validate their personnel as HSIN users. Additionally, HSIN Program Management Office representatives will work with State and local information sharing and intelligence fusion and analysis center participants to develop solutions to successfully integrate or achieve interoperability among HSIN and any applicable, existing information systems. For additional information on HSIN and available technical assistance, contact the HSIN Help Desk at (703) 674-3003.

Figure 2. Currently Available HSIN Communities of Interest (COI)

COI	Description
Counterterrorism (HSIN-CT)	Enables Federal, State, local, or tribal government agencies to share information relating to counterterrorism and incident management.
Critical Infrastructure Warning Information Network (CWIN)	A network within HSIN that provides mission-critical, survivable connectivity for DHS, SSAs, HSAs, Emergency Operations Centers (EOCs), and private sector entities vital to restoring the Nation's CI/KR.
Critical Sector (HSIN-CS)	A collection of portals established by DHS/IP to support and encourage information sharing and collaboration by the private sector within each CI/KR sector, across the sectors, and between the sectors and the government.

Emergency Management (HSIN-EM)	Enables information sharing between emergency management personnel at the Federal, State, local, and tribal levels, including EOCs.
Intelligence	Enables information sharing between authorized users in the intelligence community. Initially being used as a DHS/Office of Intelligence & Analysis (OI&A) Intranet.
International	Enables information sharing between international partners requiring close coordination with the NOC.
Law Enforcement (HSIN-LE)	Enables information sharing between all Federal, State, local, and tribal departments requiring access to Law Enforcement Sensitive information. COI members must meet the DOJ definition of law enforcement.
Law Enforcement–Analysis (JRIES LE-A)	Enables information sharing between law enforcement departments that have major Intelligence centers and are approved by the Joint Regional Information Exchange System (JRIES) Board.
Other COIs	HSIN provides the capability to develop additional temporary or permanent COIs on an as-needed basis. Examples include HSIN National Special Security Events (NSSE) and HSIN National Capital Region (NCR).
US-CERT (HSIN-US-CERT)	A focal point for communicating and addressing cyber security incidents and other relevant cyber information within the Federal government.
US Public, Private, Partnership (US P3)	Designed, implemented, and deployed as a regionally coordinated private and public information exchange and alerting forum.

- ***GSA's Cooperative Purchasing Program***
  The U.S. General Services Administration (GSA) offers an efficient and effective procurement tool for State and local governments to purchase information technology products and services to fulfill homeland security and other needs. The 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. The Cooperative Purchasing program allows for State and local governments to purchase from Schedule 70 (the Information Technology Schedule) and the Consolidated Schedule (containing IT Special Item Numbers) **only**. 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 3,000 GSA Schedule contractors who have voluntarily modified their contracts to participate in the Cooperative Purchasing program. GSA provides a definition of State and local governments as well as other vital information under the frequently asked questions section on its website at www.gsa.gov/cooperativepurchasing. The term "State and local governments"

does not include contractors of, or grantees of, the Federal, State, or local governments not otherwise named in the approved list of entities.

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

C. Application Requirements

The following steps must be completed using the on-line **http://www.grants.gov** system to ensure a successful application submission:

1. Application Process

Select "Apply for Grants," and then select "Download Application Package." Enter the Catalog of Federal Domestic Assistance (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." NOTE: You will not be able to download the Application Package unless you have installed PureEdge Viewer. The application package will be available on Grants.gov and must be submitted through that website. We recommend you visit Grants.gov prior to filing your application to fully understand the process and requirements. If you encounter difficulties, please contact the Grants.gov Help Desk at 1-800-518-4276 to report the problem and obtain assistance with the system. To use Grants.gov, the applicant, must have a Dun and Bradstreet (D&B) Data Universal Numbering System (DUNS) number[3] and register in the Central Contractor Registry (CCR). You should allow a minimum of five days to complete the CCR registration. Applications must be submitted to Grants.gov no later than **30 days after the application is posted**. DHS/G&T will evaluate and act on applications within 60 days of the application deadline.

2. Online Application

Applicants must complete the following for the FY 2006 BZPP application:

SF-424 Grant Application with Certifications

- Non-Supplanting Certification
- Assurances
- Certifications Regarding Lobbying; Debarment, Suspension, and

[3] Applicants can receive a DUNS number at *no cost* by calling the dedicated toll-free DUNS Number request line at 1-800-333-0505.

- Other Responsibility Matters; and Drug-Free Workplace Requirement

Review of Application by the State Single Point of Contact (SPOC)

The program title listed in the CFDA at http://12.46.245.173/cfda/cfda.html is *"Buffer Zone Protection Program."* The CFDA number for FY 2006 BZPP is 97.078. When completing the online application, applicants should identify their submissions as new, non-construction applications. The project period will be for a period not to exceed 24 months.

3. Consideration of Impact on Communities, Public Health, or the Environment

Federal laws, such as the National Environmental Policy Act (NEPA), require DHS to evaluate whether activities under the BZPP have the potential to have an adverse impact on communities, public health, or the environment. Projects that may have a significant adverse impact on communities, public health, or the environment will not be eligible for funding under the FY 2006 BZPP. Responsible jurisdictions must complete a checklist to provide assurances that their proposed equipment purchases will not have a significant adverse impact on communities, public health, or the environment.

NEPA, 42 USC§§4321-4370d and other Federal laws require, among other things, that Federal agencies consider the impacts of their activities on communities, public health, and the environment. In order to fulfill these requirements, DHS requires awardees and/or responsible jurisdiction sub-awardees, pursuant to the Assurances related to this grant program, to submit responses to questions regarding the awardees proposed expenditures. Applicants are required to submit a brief explanation supporting each response of "yes" or "no". Responsible jurisdiction sub-awardees with multiple expenditures must address the cumulative impact of the activities. Based on the responses to the checklist, grantees may be required to provide additional detailed information on the activities to be conducted, locations, sites, possible expenditures, possible alternatives, and any environmental concerns that may exist. This review could result in an equipment purchase not being approved for funding.

Additionally, eligible BZPP purchases must be capable of functioning independently to reduce their related vulnerabilities. BZPP purchases may not be dependent on the availability of other resources and the availability of other resources must not be dependent upon the availability of BZPP resources to fulfill their intended purposes. However, the use of other resources is encouraged to reduce the vulnerabilities identified through the BZP.

4. Compliance with Federal Civil Rights Laws and Regulations

Grantees are required to comply with Federal civil rights laws and regulations. Specifically, grantees are required to provide assurances as a condition for receipt of Federal funds from DHS that its programs and activities comply with the following:

- *Title VI of the Civil Rights Act of 1964, as amended, 42. U.S.C. 2000 et. seq.* – no person on the grounds of race, color or national origin will be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination in any program or activity receiving Federal financial assistance.
- *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. Grantees are also required to submit information, as required, to the DHS Office for Civil Rights and Civil Liberties concerning compliance with these laws and their implementing regulations.

5. Financial Requirements

1. **SF-424 Grant Application with Certifications**

   - **Non-Supplanting Certification:** The SAA may be required to affirm that Federal funds will only be used to supplement existing funds and will not replace (supplant) funds that have been appropriated for the same purpose. Potential supplanting may be addressed in the application review as well as in the pre-award review, post-award monitoring, and audit. 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.

   - **Match Requirement:** There is no match requirement.

   - **Assurances:** The applicant must comply with the list of assurances in order to receive Federal funds under this program. It is the responsibility of the recipient of the Federal funds to fully understand and comply with these requirements. Failure to comply may result in the withholding of funds, termination of the award, or other sanctions. The applicant agrees to these assurances upon the submission of the application.

   - **Certifications Regarding Lobbying; Debarment, Suspension, and Other Responsibility Matters; and Drug-Free Workplace Requirement:** This

certification, which is a required component of the application, commits the applicant to compliance with the certification requirements under 28 Code of Federal Regulations (CFR) part 67, *Government-wide Debarment and Suspension (Non-procurement);* 6 CFR part 9, *New Restrictions on Lobbying*, and 28 CFR part 83 *Government-wide Requirements for Drug-Free Workplace (Grants)*. All of these regulations can be referenced at http://www.gpoaccess.gov/cfr/index.html. The certification will be treated as a material representation of the fact upon which reliance will be placed by DHS in awarding grants.

- **Suspension or Termination of Funding:** DHS, by written notice, may terminate this grant, in whole or in part, when it is in the Government's interest.

2. **Single Point of Contact (SPOC) Review:** Executive Order 12372, located at http://www.archives.gov/federal-register/codification/executive-order/12372.html 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. The date that the application was sent to the SPOC or the reason such submission is not required should be provided.

Applicants must familiarize themselves with the requirements and restrictions of the Program Guidance for the FY 2006 BZPP and the DHS/G&T OGO Financial Management Guide. All grant recipients are assumed to have read, understood, and accepted the Program Guidance as binding.

6. 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, and religion, national origin, and sex in the delivery of services. National origin discrimination includes discrimination on the basis of limited English proficiency. To ensure compliance with Title VI, grantees 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. Because grantees are required to provide meaningful access to LEP persons in their programs and activities, grantees are 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.

7. Integrating Individuals with Disabilities into Emergency Planning

Executive Order #13347, entitled "Individuals with Disabilities in Emergency Preparedness" and signed in July 2004, requires the Federal government to support safety and security for individuals with disabilities in situations involving disasters, including earthquakes, tornadoes, fires, floods, hurricanes, and acts of terrorism. Consequently, Federal agencies are required to: 1) encourage consideration of the unique needs of persons with disabilities in emergency preparedness planning; and 2) facilitate cooperation among Federal, State, local, and Tribal governments, private organizations, NGOs, and the general public in the implementation of emergency preparedness plans as they relate to individuals with disabilities. A January 2005 letter to Governors from then-Homeland Security Secretary Tom Ridge asked States to consider several steps in protecting individuals with disabilities:

- Ensure that State's existing emergency preparedness plans are as comprehensive as possible with regard to the issues facing individuals with disabilities.
- Ensure that emergency information and resources are available by accessible means and in accessible formats.
- Consider expending Federal homeland security dollars on initiatives that address and/or respond to the needs of individuals with disabilities for emergency preparedness, response, and recovery.

Further information can be found at the Disability and Emergency Preparedness Resource Center at www.dhs.gov/disabilitypreparedness. This resource center provides information to assist emergency managers in planning and response efforts related to people with disabilities. All grantees should be mindful of Section 504 of the Rehabilitation Act of 1973 that prohibits discrimination based on disability by recipients of Federal financial assistance.

8. Freedom of Information Act (FOIA)

DHS recognizes that much of the information submitted in the course of applying for funding under this program, or provided in the course of its grant management activities, may be considered law enforcement sensitive or otherwise important to national security interests. This may include threat, risk, and needs assessment information and discussions of demographics, transportation, public works, industrial and public health infrastructures. While this information under Federal control is subject to requests made pursuant to the FOIA, 5. USC §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. Applicants are encouraged to consult their 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. Applicants may also consult their G&T Program Manager regarding concerns or questions about the release of information under state and local laws. Grantees should be familiar with the regulations governing PCII (6 CFR Part 29) and Sensitive Security Information (49 CFR Part 1520), as these designations may provide additional protection to certain classes of homeland security information.

9. 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). In geospatial systems, this location information is often paired with detailed information about the location such as: purpose/use, status, capacity, engineering schematics, operational characteristics, environmental and situational awareness. State and local emergency organizations are increasingly incorporating geospatial technologies and data to prevent, protect against, respond to, and recover from terrorist activity and incidents of national significance. In the preparedness phase, homeland security planners and responders need current, accurate, and easily accessible information to ensure the readiness of teams to respond.

Also an important component in strategy development is the mapping and analysis of critical infrastructure vulnerabilities, and public health surveillance capabilities. Geospatial information can provide a means to prevent terrorist activity by detecting and analyzing patterns of threats and possible attacks, and sharing that intelligence. During response and recovery, geospatial information is used to provide a dynamic common operating picture, coordinated and track emergency assets, enhance 911 capabilities, understand event impacts, accurately estimate damage, locate safety zones for quarantine or detention, and facilitate recovery. Use of Federal homeland security dollars for geospatial activities requires pre-approval and a demonstrated capability for robust interoperability with DHS and other relevant systems. G&T will coordinate review of requests for use of Federal homeland security funding for other geospatial projects with relevant entities.

V. Assistance, Resources and Support

A. Drawdown and Expenditure of Funds

G&T's OGO will provide fiscal support of the grant programs included in this solicitation, with the exception of payment related issues. For financial and administrative questions, all grant and sub grant recipients should refer to the OGO *Financial Management Guide* or contact OGO at 1-866-9ASK-OGO or ask-ogo@dhs.gov. All payment related questions should be referred to OJP/OC's Customer Service at 1-800-458-0786 or askoc@ojp.usdoj.gov.

Recipient organizations 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 drawdown funds up to 120 days prior to expenditure/disbursement, in response to the recommendation of the Funding Task Force. DHS strongly encourages recipients to drawdown funds as close to expenditure as possible to avoid accruing interest. ***Funds received by grantees must be placed in an interest-bearing account and are subject to the rules outlined in the Uniform Rule 28 CFR Part 66, Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments***, available at: http://www.access.gpo.gov/nara/cfr/waisidx_04/28cfrv2_04.html The Uniform Rule 28 CFR Part 70, Uniform Administrative Requirements for Grants and Agreements (Including Subawards) with Institutions of Higher Education, Hospitals and other Non-profit Organizations, at: http://www.access.gpo.gov/nara/cfr/waisidx_04/28cfrv2_04.html. These guidelines state that entities are required to promptly, but at least quarterly, remit interest earned on advances to:

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

Please consult the OGO *Financial Management Guide* or the applicable OMB Circular for additional guidance.

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

B. Centralized Scheduling and Information Desk (CSID) Help Line

The CSID is a non-emergency resource for use by emergency responders across the Nation. CSID is a comprehensive coordination, management, information, and scheduling tool developed by DHS through G&T for homeland security terrorism preparedness activities. A non-emergency resource for use by State and local emergency responders across the nation, the CSID provides general information on all G&T programs and information on the characteristics and control of CBRNE, agriculture, cyber materials, defensive equipment, mitigation techniques, and available Federal assets and resources. The CSID maintains a comprehensive database containing key personnel contact information for homeland security terrorism preparedness programs and events. These contacts include personnel at the Federal, State and local levels.

The CSID can be contacted at 1-800-368-6498 or askcsid@dhs.gov.
CSID hours of operation are from 8:00 am–7:00 pm (EST), Monday-Friday.

C. Office of Grant Operations (OGO)

G&T's OGO will provide fiscal support and fiscal oversight of the grant programs included in this solicitation. All grant and sub grant recipients should refer to the OGO *Financial Management Guide*, available at http://www.dhs.gov/dhspublic/display?theme=18.

OGO can be contacted at 1-866-9ASK-OGO or by email at ask-OGO@dhs.gov.

D. BZPP Technical Assistance Workshops

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

E. Homeland Security Technical Assistance Programs

DHS' technical assistance program seeks to build and sustain State and local jurisdiction capacity related to overall homeland security grant management. This approach ensures that technical assistance services measurably contribute to the

enhancement of the homeland security grant architecture within each State and local jurisdiction, as well as the associated preparedness capabilities housed therein.

In FY 2006, G&T will release the Homeland Security Virtual Assistance Center (HSVAC) which will provide an on-line resource for grantees to access technical assistance offerings. For additional information, see G&T's online TA site at http://www.ojp.usdoj.gov/odp/ta.htm under the *Catalog* link or contact the CSID.

F. Lessons Learned Information Sharing (LLIS) System

LLIS is a national, online, secure website that houses a collection of peer-validated lessons learned, best practices, and After Action Reviews (AAR) 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 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 located at https://www.llis.gov.

G. Equipment Purchase Assistance Program

The Equipment Purchase Assistance Program provides G&T grantees with access to prime vendors through memoranda of agreement with the Defense Logistics Agency (DLA). Benefits of the program include shorter procurement lead time, online ordering, a diverse inventory of commercial products, and seven-day delivery for routine items. When ordering equipment through this program, grantees may only use funds awarded by G&T; State and local funds may not be used. Establishing an account with DLA is a straightforward process that should be initiated by contacting the appropriate program representative. Additional information on the programs and contact information for program representatives is available in a fact sheet posted on the G&T website at http://www.ojp.usdoj.gov/odp/docs/fs-padef.htm.

VI. Reporting, Monitoring and Closeout Requirements

A. Reporting and Closeout Requirements

As required under the Government Performance and Results Act (GPRA), DHS collects and reports performance information across all of its programs, including grant programs. For grant programs, assessing performance information allows the Department to ensure that grant funds are achieving positive, measurable progress in improving national preparedness. The Department uses general information from grant programs to report on the following performance measures:

- Percent of State and local homeland security agency grant recipients reporting measurable progress towards identified goals and objectives to prevent and respond to terrorist attacks.
- Percent progress toward implementation of State strategies observed by Preparedness Officers.
- Percent of participating Urban Area grant recipients reporting measurable progress made towards identified goals and objectives to prevent and respond to terrorist attacks.
- Percent progress toward State strategies implementation for Urban Area Grant Recipients observed by Preparedness Officers.

To collect and report on these measures, the Department will the following information: general information from State Strategies, Biannual Strategy Implementation Reports, and Grant Monitoring Reports. Please note that the Department does not use this general performance information as a basis for awarding State and local grants; rather, the Department uses the information to assess overall program effectiveness and impact, and to report results to Congress, the Office of Management and Budget (OMB), and the President.

B. Grant Award and Obligation of Funds

Upon approval of the application, the grant will be awarded to the respective SAA. This date will be known as the "award date." The signed award document with special conditions must be returned to the OJP Control Desk. See Appendix A for additional information and mailing address. **The State's obligation period must be met within 60 days of the approval notification for the VRPP under the BZPP.** An obligation is defined as a definite commitment which creates a legal liability for the payment of funds for goods and services ordered or received. Five requirements must be met to obligate grant funds:

- There must be some action to establish a firm commitment on the part of the awarding entity.
- The condition must be unconditional 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 approval of the drawdown on funds for a VRPP must be communicated by DHS to the official grantee.

Within 60 days of the approval notification for the VRPP, the SAA will submit a certification that funds have been passed through to local units of government (to include the identification of subgrantees and sub-award amounts.)

C. Drawdown of Funds

Following the acceptance of the grant award and the release of any special conditions withholding funds, the grantee can drawdown funds through the following methods: the ASAP, PAPRS, or LOCES.

In support of continuing efforts to meet the accelerated financial statement reporting requirements mandated by the U.S. Department of the Treasury and OMB, payment processing will be interrupted during the last five (5) working days of each month. SAAs should make payment requests before the last five working days of the month to avoid delays in deposit of payments. For example, for the month of September, the last day to request (drawdown) payments was September 23, 2006. Payments requested after September 23, 2006, will be processed when the regular schedule resumed on October 1, 2006. A similar schedule will follow at the end of each month thereafter.

To avoid denial of payment requests, grantees are encouraged to submit their SF269a FSRs online at http://grants.ojp.usdoj.gov. Additional information and instructions are available at this website.

Questions regarding grant payments should be addressed to the OJP OC at 1-800-458-0786 or email askoc@ojp.usdoj.gov.

Questions regarding all other financial/administrative issues should be addressed to the OGO Information Line at 1-866-9ASKOGO (927-5646) or email at ask-ogo@dhs.gov.

D. Reporting Requirements

Reporting requirements for all programs included in BZPP will be consolidated into a single reporting system.

1. Financial Status Report (FSR) (Required quarterly)

Obligations and expenditures must be reported to G&T on a quarterly basis through the FSR, which is due within 30 days of the end of each calendar quarter (e.g., for the quarter ending March 31, FSR is due on April 30). Please note that this is a change from previous fiscal years. A report must be submitted for every quarter the award is active, including partial calendar quarters, as well as for periods where no grant activity

occurs. FSRs must be filed online at http://grants.ojp.usdoj.gov. Future awards and fund drawdowns will be withheld if these reports are delinquent.

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

- OMB Circular A-102, *Grants and Cooperative Agreements with State and Local Governments*, at http://www.whitehouse.gov/omb/circulars/index.html.
- OMB Circular A-87, *Cost Principles for State, Local, and Indian Tribal Governments,* at http://www.whitehouse.gov/omb/circulars/index.html.
- OMB Circular A-110, *Uniform Administrative Requirements for Grants and Other Agreements with Institutions of Higher Education, Hospitals and Other Non-Profit Organizations*, at http://www.whitehouse.gov/omb/circulars/index.html.
- OMB Circular A-21, *Cost Principles for Educational Institutions,* at http://www.whitehouse.gov/omb/circulars/index.html.
- OMB Circular A-122, *Cost Principles for Non-Profit Organizations,* at http://www.whitehouse.gov/omb/circulars/index.html.

For FY 2006 awards, grant and sub-grant recipients should refer to the OGO Financial Management Guide. All previous awards are still governed by the OJP Financial Guide, available at http://www.ojp.usdoj.gov/FinGuide. OGO can be contacted at 1-866-9ASKOGO or by email at ask-OGO@dhs.gov.

2. Biannual Strategy Implementation Reports (BSIR) and Categorical Assistance Progress Report (CAPR)

Following award of grant, the State and subgrantees will be responsible for providing updated obligation and expenditure information on a regular basis. States will provide consolidated information to G&T in their BSIR. The BSIR submission will satisfy the narrative requirement in Box 12 of the biannual CAPR (OJP Form 4587/1). States will still be required to submit the CAPR form with a line in box 12 which reads: See BSIR. The CAPR must be filed online at http://grants.ojp.usdoj.gov.

The BSIR and the CAPR are due within 30 days after the end of the reporting period (July 31 with a reporting period of January 1 through June 30, and on January 31 with a reporting period of July 1 though December 31). Updated obligation and expenditure information must be provided with the BSIR to show progress made toward meeting strategic goals and objectives. G&T will provide a web-enabled application for the BSIR submission to grantees. Future awards and fund drawdowns may be withheld if these reports are delinquent. The final BSIR is due 90 days after the end date of the award period.

3. Financial and Compliance Audit Report

Recipients that expend $500,000 or more of Federal funds during their fiscal year are required to submit an organization-wide financial and compliance audit report. The audit

must be performed in accordance with the Government 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/index.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 2006 BZPP assistance for audit and examination purposes, provided that, in the opinion of the Secretary of Homeland Security or the Comptroller General, these documents are related to the receipt or use of such assistance. The grantee will also give the sponsoring agency or the Comptroller General, through any authorized representative, access to, and the right to, examine all records, books, papers or documents related to the grant.

The State shall require that subgrantees 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.

E. Monitoring

Grant recipients will be monitored periodically by the Preparedness Directorate for substantive program management and for grant management to ensure that the program goals, objectives, timeliness, budgets, and other related program criteria are being met. Monitoring is accomplished through a combination of office-based and on-site monitoring visits. Monitoring involves the review and analysis of the financial, programmatic, and administrative issues relative to each program, and helps identify areas where technical assistance and other support may be needed. Beginning in FY 2006, the Preparedness Directorate will conduct financial monitoring of all States and Urban Areas during the grant period.

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

F. Grant Close-Out Process

Within 90 days after the end of the award period, the grantee will submit a final FSR, final CAPR, and final BSIR detailing all accomplishments throughout the project. Please note that this is a change from previous fiscal years. After these reports have been reviewed and approved by the G&T Preparedness Officer, a Grant Adjustment Notice (GAN) will be completed to close-out the grant. The GAN will indicate the grant as being closed, list any remaining funds that will be de-obligated, 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 the OGO, the grant will be identified as “Closed by the Office of Grant Operations.”

APPENDIX A

AUTHORIZED PROGRAM EXPENDITURES GUIDANCE

Authorized Program Expenditures Guidance

A. Allowable Costs Guidance

This section provides guidance on the types of expenditures that are allowable under the FY 2006 BZPP. Please refer to the checklist in Appendix C for a summary of authorized and unauthorized BZPP expenditures. Grantees are encouraged to contact their G&T Preparedness Officer regarding authorized and unauthorized expenditures.

Planning

Planning activities are central to the implementation of the BZPP. Accordingly, local jurisdictions may use up to 15% of BZPP programmatic funds to support multi-discipline planning activities. These funds will support local jurisdictions in building capabilities, updating preparedness strategies, developing CIP programs, allocating resources, and delivering preparedness programs across jurisdictions, disciplines (e.g., law enforcement, fire, EMS, public health, public works, and information technology) and levels of government. These efforts include the collection and analysis of intelligence and information and the development of policies, plans, procedures, mutual aid agreements, strategies, and other publications that comply with relevant laws, regulations, and guidance necessary to perform assigned missions and tasks. The planning process should also address emergency operations plans and protocols for addressing major events and program planning in coordination with each State's CIP program, as a component of the State homeland security program.

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

FY 2006 BZPP funds may be used for a range of homeland security and critical infrastructure planning activities, such as:

- Developing and implementing homeland security and critical infrastructure support programs and adopting DHS national initiatives limited to the following:
    - Implementing the NPG, as it relates to implementation of the NIPP, and sector specific plans.
    - Modifying existing incident management and Emergency Operating Plans (EOPs) to ensure proper alignment with the National Response Plan (NRP) and the National Incident Management System (NIMS) coordinating structures, processes, and protocols.
    - Establishing or enhancing mutual aid agreements or MOUs to ensure cooperation with respect to CIP.
    - Developing communications and interoperability protocols and solutions.
    - Developing or updating resource inventory assets in accordance to typed resource definitions issued by the NIC.

  - Designing State and local geospatial data systems.

- Developing related terrorism prevention and protection programs including:
  - Planning to enhance security during heightened alerts, during terrorist incidents, and/or during mitigation and recovery.
  - Multi-discipline preparation across the homeland security community.
  - Developing and planning for information/intelligence sharing groups.
  - 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.

Equipment

Through the FY 2006 BZPP, only select Authorized Equipment List (AEL) categories are eligible for funding (see Table 1 below). The allowable equipment categories are listed on the web-based AEL on the Responder Knowledge Base (RKB), which is sponsored by G&T and the National Memorial Institute for the Prevention of Terrorism (MIPT) at http://www.rkb.mipt.org.

The FY 2006 AEL is housed on the RKB along with separate listings for the FY 2005 AEL and the Fall 2005 Standardized Equipment List (SEL). In some cases, items on the SEL are not allowable under FY 2006 BZPP, or will not be eligible for purchase unless specific conditions are met. In addition, some new items that are eligible under FY 2006 BZPP are not available for purchase with FY 2005 funds. During the course of FY 2006, G&T will highlight significant updates to the AEL in real time on the RKB. These updates will be noted in a change log posted on the main page of the AEL within the RKB. Grantees should also refer to the notes included in each equipment item entry within the selected AEL categories for additional information on these changes and their impact on eligibility.

Any questions or suggestions concerning the eligibility of equipment not addressed in the AEL should be directed to the appropriate G&T Preparedness Officer. The “Other Authorized Equipment” category on the AEL contains a number of equipment-related costs, such as sales tax, leasing of space, installation, and maintenance. Grantees should refer to that section for specific guidance. Unless otherwise specified, maintenance costs/contracts for authorized equipment purchased using FY 2006 BZPP

funding or acquired through G&T's Homeland Defense Equipment Reuse (HDER) Program are allowable.

As required by the FY 2006 DHS Appropriations Conference Report, if States plan to purchase interoperable communications equipment, they must certify to G&T that they have an implementation plan for the equipment that includes governance structures, policies, procedures, training, and planned exercises to ensure that key elements of planning, governance, and training are addressed before the equipment is procured.

The AEL categories eligible for funding under the FY 2006 BZPP are available online through the RKB at http://www.rkb.mipt.org and the **only** allowable equipment categories under the FY 2006 BZPP are outlined in Table 2 below and Appendix B.

Table 2. BZPP Allowable Equipment Categories

#	Category Title
[2]	Explosive Device Mitigation and Remediation Equipment
[3]	CBRNE Operational Search and Rescue Equipment*
[4]	Information Technology
[5]	Cyber Security Enhancement Equipment
[6]	Interoperable Communications Equipment
[7]	Detection Equipment
[10]	Power Equipment
[13]	Terrorism Incident Prevention Equipment
[14]	Physical Security Enhancement Equipment
[15]	Inspection and Screening Systems
[16]	Agricultural Terrorism Prevention, Response and Mitigation Equipment
[21]	Other Authorized Equipment

* Only select sub-categories within AEL Category 3 are eligible for FY 2006 BZPP funding. These sections include: 3.1.6, 3.2.2, 3.2.3, and 3.2.4.

Management and Administrative (M&A) Costs

No more than 5 percent of the total State award under FY 2006 BZPP may be used for M&A by the State. Local jurisdiction subgrantees may retain and use up to 3 percent of their subaward from the State for local M&A purposes. States may pass through a portion of the State M&A allocation to local subgrantees in order to supplement the 3 percent M&A allocation allowed on subgrants. However, no more than 5 percent of the total subaward may be expended by subgrantees on M&A costs. Please consult the DHS/G&T OGO Financial Management Guide for additional guidance on M&A costs.

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 of the FY 2006 BZPP.
  - To assist with the development, implementation, and requirements of the FY 2006 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 2006 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 2006 BZPP.

B. Unallowable Costs Guidance

Funding from the FY 2006 BZPP is reserved for the acquisition and use of the allowable materials, equipment, and resources identified in the VRPP, as necessary, to implement preventive and protective measures that will reduce vulnerabilities and/or increase capabilities of the jurisdiction around identified CI/KR sites. A limited amount of FY 2006 BZPP funding may be used to support M&A activities (see allowable M&A costs guidance on page 24) directly related to FY 2006 BZPP implementation.

1. Hiring of Public Safety Personnel. FY 2006 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. See also Appendix C for allowable hiring expenditures.

2. Construction and Renovation. Construction and renovation is prohibited under the FY 2006 BZPP.

3. 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.

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

5. Training and Exercise Activities. Any resulting training or exercise requirements identified through the BZPP may not be funded with FY 2006 BZPP funds, but may be funded through other overarching homeland security grant programs (i.e. SHSP, UASI, and/or LETPP funds) 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 preparedness capabilities directed at chemical sector facilities and/or the surrounding communities
- The development of risk/vulnerability assessment models
- Initiatives that fund risk or vulnerability security assessments or the development of BZPs and/or VRPPs
- Initiatives in which Federal agencies are the beneficiary or that enhance Federal property
- Initiatives which study technology development
- Proof-of-concept initiatives
- Initiatives that duplicate capabilities being provided by the Federal government
- Operating expenses
- Reimbursement of pre-award security expenses
- Other indirect costs

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

APPENDIX B

HISTORICAL ALLOWABLE DATA

Historical Allowable Data

The following tables show how allowable costs have changed since FY 2005 for the various G&T BZPP grant programs under the categories of Planning, Equipment (AEL Categories), and Management and Administration. Please review the grant guidance for specific allowable activities under each category.

Table 3. Historical Planning Categories

	FY 2005	FY 2006
Planning Costs	**BZPP**	**BZPP**
Implementing and managing programs for equipment acquisition, training and exercises		Y
Develop and enhance plans and protocols		Y
Develop or conduct assessments		
Develop and implement homeland security support programs and adopt ongoing DHS national initiatives		Y
Materials and Meeting Related Expenses		Y
Hiring of full or part-time staff or contractors/consultants to assist with any related planning activities (not for the purpose of hiring public safety personnel)		Y

Table 4. Historical Equipment Costs

		FY 2005	FY 2006
Authorized Equipment List Categories		**BZPP**	**BZPP**
1	Personal Protective Equipment	Y	
2	Explosive Device Mitigation and Remediation Equipment	Y	Y
3	CBRNE Operational and Search & Rescue Equipment	Y	Y*
4	Information Technology	Y	Y
5	Cyber Security Enhancement Equipment	Y	Y
6	Interoperable Communications Equipment	Y	Y
7	Detection Equipment	Y	Y
8	Decontamination Equipment	Y	
9	Medical Supplies and Limited Types of	Y	

* Only select sub-categories within AEL Category 3 are eligible for FY 2006 BZPP funding. These sections include: 3.1.6, 3.2.2, 3.2.3, and 3.2.4.

		FY 2005	FY 2006
	Authorized Equipment List Categories	BZPP	BZPP
	Pharmaceuticals		
10	Power Equipment	Y	Y
11	CBRNE Reference Materials	Y	
12	CBRNE Incident Response Vehicles	Y	
13	Terrorism Incident Prevention Equipment	Y	Y
14	Physical Security Enhancement Equipment	Y	Y
15	Inspection and Screening Systems	Y	Y
16	Agricultural Terrorism Prevention, Response and Mitigation Equipment	Y	Y
17	CBRNE Prevention and Response Watercraft	Y	
18	CBRNE Aviation Equipment	Y	
19	CBRNE Logistical Support Equipment	Y	
20	Intervention Equipment	Y	
21	Other Authorized Equipment	Y	Y

Table 5. Historical Management & Administrative Costs

	FY 2005	FY 2006
Management & Administrative Costs	BZPP	BZPP
Meeting-related expenses	Y	Y
Development of operating plans for information collection and processing necessary to respond to G&T data calls	Y	Y
Hiring part-time staff or contractors/consultants to assist with management, implementation and administration	Y	Y
Overtime and backfill	Y	
Travel	Y	Y
Leasing and/or renting of office space for newly hired personnel	Y	Y
Recurring fees/charges associated with certain equipment, such as cell phones, faxes, etc. (allowable only within the period of performance of the grant program)	Y	Y
Acquisition of authorized office equipment (includes personal computers, laptops, printers, LCD projectors and other equipment or software which may be required to support implementation of the State strategy)	Y	Y

	FY 2005	FY 2006
Management & Administrative Costs	**BZPP**	**BZPP**
The percentage of the program that may be used for M&A	3%	5%
Percentage of grant program that may be subawarded from the State for local M&A purposes	3%	3%
Pass-through Requirements	97%	95%

APPENDIX C

RELATIONSHIP OF BZPP GRANT PROGRAMS TO TARGET CAPABILITIES

Relationship of BZPP Grant Programs to Target Capabilities

Grant programs link to the Target Capabilities according to the following table. "Y" denotes a direct role for the capability, while "*" denotes a supporting role or collateral capability.

Table 6. – Relationship of Grants to Target Capabilities

37 Target Capabilities and Categories	BZPP
Common Target Capabilities	
Planning	Y
Community Preparedness and Participation	Y
Communications	Y
Risk Management	Y
Prevent Mission Area Target Capabilities	
Info Gathering and Recognition of Indicators and Warnings	Y
Law Enforcement Investigation and Operations	Y
Intelligence Analysis and Production	Y
CBRNE Detection	Y
Intelligence / Information Sharing and Dissemination	Y
Protect Mission Area Target Capabilities	
Critical Infrastructure Protection	Y
Epidemiological Surveillance & Investigation	Y
Public Health Laboratory Testing	Y
Food and Agriculture Safety and Defense	Y
Respond Mission Area Target Capabilities	
Onsite Incident Management	*
Citizen Protection: Evacuation and/or In-Place Protection	*
Emergency Operations Center Management	*
Isolation and Quarantine	
Critical Resource Logistics and Distribution	*
Urban Search & Rescue	
Volunteer Management and Donations	
Emergency Public Information and Warning	*

Responder Safety and Health	
Triage and Pre-Hospital Treatment	
Public Safety and Security Response	*
Medical Surge	
Animal Health Emergency Support	
Medical Supplies Management and Distribution	
Environmental Health	
Mass Prophylaxis	
Explosive Device Response Operations	*
Mass Care	
Firefighting Operations/Support	
Fatality Management	
WMD/Hazardous Materials Response and Decontamination	*
Recover Mission Area Target Capabilities	
Structural Damage and Mitigation Assessment	*
Economic & Community Recovery	*
Restoration of Lifelines	*

APPENDIX E

GRANTS.GOV QUICK-START INSTRUCTIONS

Grants.gov Quick-Start Instructions

G&T is participating in the e-Government initiative, one of 25 initiatives included in the President's Management Agenda. Grants.gov, part of this initiative, is a "storefront" that provides a unified process for all customers of Federal grants to find funding opportunities and apply for funding. This fiscal year, G&T is requiring that all discretionary, competitive grant programs be administered through 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.

- **Step 1: Registering**

  Note: 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 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.

  e-Business Point of Contact
  Grants.gov requires an organization to first be registered in the Central Contract Registry (CCR) before beginning the Grants.gov registration process. If you plan to authorize representatives of your organization to submit grant applications through Grants.gov, proceed with the following steps. If you plan to submit a grant application yourself and sign grant applications and provide the required certifications and/or assurances necessary to fulfill the requirements of the application process, proceed to DUNS Number and then skip to the Authorized Organization Representative and Individuals section.
  Go to www.grants.gov, and click on the "Get Started" tab at the top of the screen.

  - Click the "e-Business Point of Contact (POC)" 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.

DUNS Number

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

Central Contractor Registry (CCR)

Note: 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/CCRRegTemplate.pdf. 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 POC is for your agency. If your organization is not already registered, return to the CCR home page and click "Start New Registration" at the top left of the screen.

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

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

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.

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 (AOR).

- Once you are logged in, go to Step 2. *Downloading the Application Viewer*, below.

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.

Credential Provider:

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

- If you should need help with this process, please contact the Credential Provider Customer Service at 1–800–386–6820.

- It can take up to 24 hours for your credential provider information to synchronize with Grants.gov. Attempting to register with Grants.gov before the synchronization is complete may be unsuccessful.

Grants.gov:

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

- Complete the "Authorized Organization Representative User Profile" screen and click "Submit."

Note: Individuals do not need to continue to the "Organizational Approval" step below.

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**

Note: 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**

Note: 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

Note: 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 are one of four status messages your application can receive in the system:

  1. **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.

  2. **Received by Agency:** This means our agency has 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.

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

  4. **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.

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

APPENDIX E

POST AWARD INSTRUCTIONS

Post Award Instructions

TAB 1: SAMPLE REVIEW OF AWARD

Office of Grants and Training
Post Award Instructions for G&T Awards

The OGO will provide fiscal support and oversight of the grant programs, while the OJP Office of the Comptroller will continue to provide support for grant payments. The following is provided as a guide for the administration of awards.

1. Review Award and Special Conditions Document.

Notification of award approval is made by e-mail through the OJP Grants Management System (GMS). Once an award has been approved, a notice is sent to the e-mail address of the individual who filed the application, as well as to the authorized grantee official.

Carefully read the award and any special conditions or other attachments.

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

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

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

2. Read Guidelines.

Read and become familiar with the "*OGO Financial Management Guide*" which is available at 1-866-9ASKOGO or online at http://www.dhs.gov/dhspublic/display?theme=18.

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

4. Access to Payment Systems.
OJP uses two payment systems: PAPRS and LOCES (refer to Step 4 attachment). Current LOCES users will see the addition of new grants on the LOCES grant number listing as soon as the award acceptance has been received. PAPRS grantees will receive a letter with the award package containing their PIN to access the system and Grant ID information.

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

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

***Important 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 Hotline at 1-888-549-9901.**

APPENDIX F

ADDITIONAL GUIDANCE ON THE NATIONAL PREPAREDNESS GOAL AND THE NATIONAL PRIORITIES

Additional Guidance on the National Preparedness Goal and the National Priorities

A. The National Preparedness Goal[5]

> ***Vision of the National Preparedness Goal***:
>
> *To engage Federal, state, local, and tribal entities, their private and non-governmental partners, and the general public to achieve and sustain risk-based target levels of capability to prevent, protect against, respond to, and recover from major events in order to minimize the impact on lives, property, and the economy.*

The Goal establishes a vision for National Preparedness, including National Priorities. The TCL further identifies 37 needed capabilities integral to nationwide all-hazards preparedness, including acts of terrorism.[6] The national preparedness doctrine and operational foundation provided in these documents form the basis for use of Federal grant funds and consistent direction among all stakeholders. The Goal is a significant evolution in securing a sustained national approach to preparedness and homeland security. The Goal is a companion document to the NRP, NIMS, and the NIPP. The Goal establishes a framework that guides entities at all levels of government in the development and maintenance of the capabilities to prevent, protect against, respond to, and recover from major events, including catastrophic events or Incidents of National Significance, as defined in the NRP. The Goal will also assist entities at all levels of government, as well as non-government entities, in the development and maintenance of the capabilities to identify, prioritize, and protect critical infrastructure and key resources as described in the NIPP. Risk and capability-based planning for prioritizing homeland security investments will be performed in accordance with the final National Preparedness Goal.

Implementing a common, shared approach to achieving national preparedness requires the Nation to orient its programs and efforts in support of the Goal and the National Priorities. The ability of Federal, state, local and tribal entities to orient their efforts begins with capabilities-based planning. The TCL defines capability-based planning as "planning, under uncertainty, to provide capabilities suitable for a wide range of threats and hazards while working within an economic framework that necessitates prioritization and choice." This planning approach assists leaders at all levels to allocate resources systematically to close capability gaps, thereby enhancing the effectiveness of preparedness efforts. Capabilities-based planning will provide a means for the Nation to achieve the Goal and National Priorities by answering three fundamental questions: "*How prepared do we need to be?*", *"How prepared are we?"*, and *"How do we prioritize efforts to close the gap?"* At the heart of the Goal and the capabilities-based planning process is the TCL. The capabilities included in the TCL are listed in Figure 3.

[5] As this grant guidance went to print, the final Goal document was also being prepared for release.
[6] This guidance references 37 capabilities based on the most recent draft of the TCL available at the time this guidance went to press.

Figure 3. Target Capabilities

37 Target Capabilities	
Common • Planning • Communications • Risk Management • Community Preparedness and Participation **Prevent Mission Area** • Information Gathering & Recognition of Indicators & Warnings • Intelligence Analysis and Production • Intelligence / Information Sharing and Dissemination • Law Enforcement Investigation and Operations • CBRNE Detection **Protect Mission Area** • Critical Infrastructure Protection (CIP) • Food & Agriculture Safety & Defense • Epidemiological Surveillance and Investigation • Public Health Laboratory Test **Recover Mission Area** • Structural Damage and Mitigation Assessment • Restoration of Lifelines • Economic & Community Recovery	**Respond Mission Area** • Onsite Incident Management • Emergency Operations Center Management • Critical Resource Logistics and Distribution • Volunteer Management and Donations • Responder Safety and Health • Public Safety and Security Response • Animal Health Emergency Support • Environmental Health • Explosive Device Response Operations • Firefighting Operations/Support • WMD/HazMat Response and Decontamination • Citizen Protection: Evacuation and/or In-Place Protection • Isolation and Quarantine • Urban Search & Rescue • Emergency Public Information and Warning • Triage and Pre-Hospital Treatment • Medical Surge • Medical Supplies Management and Distribution • Mass Prophylaxis • Mass Care (Sheltering, Feeding, and Related Services) • Fatality Management

The capabilities-based planning process makes significant use of the TCL which provides additional levels of detail on the underlying tasks and resources for achieving these capabilities. Each level of government or geographic area will not be expected to develop and maintain all 37 capabilities to the same extent. Capability-based planning requires the prioritization of resources and initiatives among the various capabilities listed in the TCL. Given a limited time and resources, jurisdictions will be expected to prioritize their planning efforts, focusing on the most critical capability gaps. The expectation will vary based upon the risk and needs of different levels of government and geographic areas.

For example, basic capability levels may be expected of a low-population jurisdiction, while a more advanced degree of capability may be expected among a group of jurisdictions, an entire state, or the Federal government. Consequently, organizational and operational integration is required across agencies, disciplines and jurisdictions – and across state lines. Mutual aid agreements, inter-organizational linkages (including authorities, agencies, non-governmental partners and individual citizens), information sharing, and collaboration that empower this integration become critical elements of the new preparedness landscape.

The Goal and the TCL are all-hazards in nature and address a range of major events, including terrorism and the capabilities required to address them. However, consistent with Congressional direction, these particular grant programs remain primarily focused on enhancing capabilities to prevent, protect against, respond to, or recover from CBRNE, sabotage, and cyber terrorism incidents. Further, these grant programs do not support all elements within each capability in the TCL. A number of additional resources at different levels of DHS and all of government are available and should be leveraged to build and sustain capabilities. For example, the Critical Infrastructure Protection Capability of the TCL recommends an appropriate number of infrastructure security specialists, however, the costs associated with hiring those personnel are not allowable under these grants.

The Goal encompasses the full spectrum of activities necessary to address the entire range of threats and hazards. In addition to a number of common activities that support preparedness (e.g., planning, interoperable communications, risk management, and citizen preparedness and participation), four mission areas help create a framework for developing the subset of national capabilities that will be supported by DHS preparedness grant program funding as well as state and local funds. The four mission areas are prevent, protect, respond, and recover. As stated in the NIMS, mitigation activities are important elements of preparedness and provide a critical foundation across the spectrum from prevention through recovery. The mission areas are discussed in further detail below.

Prevent: Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves intelligence and deterrence operations; heightened inspections; improved surveillance and security operations; investigations; education and training; enhanced nuclear and radiological detection capabilities; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and certain law enforcement operations.[7] Public announcements, infrastructure improvements and citizen vigilance also are important, especially when considering an all-hazards approach.

Protect: Actions to reduce the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks, major disasters, and other emergencies.[8] Protection also includes: continuity of government and operations planning; evacuation planning, awareness elevation and understanding of threats and vulnerabilities to related critical facilities, systems, and functions; promotion of effective sector-specific protection practices and methodologies; and expansion of voluntary security-related information sharing between government and private entities.[9]

Respond: Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human

[7] NIMS, March 2004.
[8] Homeland Security Presidential Directive-7 (HSPD-7) December 2003.
[9] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003.

needs. As indicated by the situation, response activities include: applying intelligence and other information to lessen the effects or consequences of an incident; increasing security and law enforcement operations; continuing investigations into the nature and source of the threat; continuing ongoing public health and agricultural surveillance and testing processes; providing immunizations; enforcing isolation or quarantine; and allowing appropriate citizen response.[10] A prepared community will also possess sufficient capability for emergency feeding and sheltering of displaced personnel.

Recover: The development, coordination, and execution of service and site restoration plans; the reconstitution of government operations and services; individual, private-sector, non-governmental, and public assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents.[11]

Each mission area includes a collection of capabilities that require integration and collaboration across multiple disciplines, jurisdictions, levels of government, processes, and procedures. Many of these capabilities support the achievement of the National Priorities listed in the Goal.

The Goal and the TCL are evolving documents that will be updated regularly to incorporate new threats, technologies, improvements to capability levels, new preparedness initiatives and priorities, and lessons learned. DHS will coordinate the establishment of a structure and process for the ongoing management and maintenance of the Goal. This structure and process will be coordinated closely with the ongoing management and maintenance of the NIMS, NRP, and NIPP. Such coordination will ensure that national policy and planning for operations and preparedness are mutually supportive.

The Nation's priorities, target levels, and performance metrics within the TCL will be modified to reflect the completion or update of assessments, and will include benchmarks for measuring progress. Additional foreseeable changes to the documents and their implementation will include:

- Recommendations and lessons learned from the response to Hurricane Katrina;
- Revisions to the NRP;
- Capabilities required for implementing the NIPP;
- Capabilities required for implementing the National Strategy for Pandemic Influenza;
- Prevention tasks and capabilities identified by updated National Planning Scenarios and reflective of current Administration policies on the War on Terror.

[10] NIMS, March 2004.
[11] NIMS, March 2004.

State and local governments and public safety entities are encouraged to participate in the maintenance process by submitting questions and comments related to the Goal's implementation.

B. The National Priorities

The National Priorities in the Goal help guide the Nation's preparedness efforts to meet its most urgent needs. The priorities fall into two categories: (A) Overarching priorities that contribute to the development of multiple capabilities, and (B) Capability-specific priorities that establish selected capabilities for which the Nation has the greatest need.[12] Security partners at all levels of government recently developed homeland security strategies that align with and support the overarching priorities established in the Goal.

With the inclusion of NIPP implementation as one of these overarching national priorities, CI/KR protection programs form an essential component of state, territorial, local, tribal and sector-specific homeland security strategies, particularly with regard to informing funding priorities and security investment decisions. To permit effective NIPP implementation, and use of performance measurement, these protection programs should reference all core elements of the NIPP framework, including key cross-jurisdictional security and information-sharing linkages, as well as specific CI/KR protective programs focused on risk reduction. These programs should also support DHS and sector-specific efforts to identify, ensure connectivity with, and enable the protection of CI/KR of national-level criticality within the jurisdiction.

The following section outlines each of the National Priorities, as well as critical benchmarks developed to assist DHS and grantees in demonstrating progress made toward achieving the National Priorities. The three overarching priorities are:

B.1. Expanded Regional Collaboration

Major events, especially acts of terrorism, will invariably have cross-geographic consequences and impacts. The Expanded Regional Collaboration Priority highlights the need for partnerships across multiple jurisdictions, regions, and states in building capabilities cooperatively. Successful regional collaboration allows for a multi-jurisdictional and multi-disciplinary approach to building capabilities for all four mission areas, spreading costs, and sharing risk across geographic areas. This approach increases efficiency and enhances capabilities. Regional collaboration focuses on expanding mutual aid and assistance compacts among contiguous state, local, and tribal entities, and their private and non-governmental partners, and extending the scope of those compacts to include pre-incident preparedness activities (e.g., planning, training, exercising). The intent is to tactically locate capabilities in order to maximize coverage of the U.S. population and the Nation's high priority CI/KR. The Goal establishes as a priority the embracing of regional approaches to building, sustaining, and sharing capabilities at all levels of government.

[12] One of the four capability-specific priorities, Enhance Medical Surge and Mass Prophylaxis Capabilities is not relevant to the FY 2006 DHS Infrastructure Protection Program.

B.2. Implement the NIMS and NRP

Homeland Security Presidential Directive-5 (HSPD-5), "*Management of Domestic Incidents*," mandated the creation of NIMS and NRP. The NRP establishes a comprehensive all-hazards approach to managing domestic incidents. The plan incorporates best practices and procedures from incident management disciplines – homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector – and integrates those best practices and procedures into a unified structure. The NIMS provides a consistent framework for entities at all jurisdictional levels to work together to implement the NRP and manage domestic incidents, regardless of cause, size, or complexity. To promote interoperability and compatibility among Federal, state, local, and tribal capabilities, the NIMS includes a core set of guidelines, standards, and protocols for command and management, preparedness, resource management, communications and information management, supporting technologies, and management and maintenance of NIMS.

The NRP, using the template established by the NIMS, is an all-discipline, all-hazards plan that provides the structure and mechanisms to coordinate operations for emergencies that require a coordinated Federal response. Based on the criteria established in HSPD-5, Incidents of National Significance are those high-impact events that require a coordinated and effective response by an appropriate combination of Federal, state, local, tribal, private sector, and non-governmental entities in order to save lives, minimize damage, and provide the basis for long-term community recovery and mitigation activities. DHS and other Federal agencies are currently reviewing implementation of the NRP during Hurricanes Katrina and Rita.

The implementation of the NIMS within every state, territory, tribal, and local jurisdiction creates a common framework and system that, once established nationwide, will be the foundation for prevention, protection, response, and recovery operations. Full NIMS implementation is a dynamic and multi-year phase-in process with important linkages to the NRP, HSPD-8 (i.e., the Goal) and the Interim NIPP. The NIMS Integration Center (NIC) will continue to work with Federal departments and agencies to ensure Federal implementation of NIMS and that all FY 2006 Federal preparedness assistance programs reflect and support NIMS implementation at the state, local, and tribal government levels as appropriate.

While NIMS is not a specific requirement for the ports under this grant program, States and urban areas are required to meet the FY 2006 NIMS implementation requirements as a condition of receiving Federal preparedness funding assistance next year, in FY 2007. Thus, ***transportation and other infrastructure systems participating in should review the NIMS requirements for local jurisdictions, and adopt those that are applicable.***

Major goals for this priority in FY 2006 are:

- Educate all appropriate officials on the incident management roles and responsibilities of the NIMS and NRP through awareness courses provided by DHS.
- Identify the appropriate infrastructure personnel, public-sector contacts, and protocols for connecting with relevant Federal, state, and local agencies through NIMS and the NRP in the event of an emergency.
- Integrate with existing state/local NIMS implementation strategies, as appropriate.
- Participate in Federal, state, and local exercises that are designed to test the implementation of NIMS and the NRP.

***Note*: G&T will continue to update grantees on NIMS compliance measures as they become available. Additional information about NIMS implementation and resources for achieving compliance are available through the NIC. The NIC web page, *http://www.fema.gov/nims*, is updated regularly with information about the NIMS and additional guidance for implementation.**

B.3. Implement the NIPP

Infrastructure protection is an integral part of the homeland security mission and overall national preparedness efforts. A key element of the national approach to infrastructure protection is the NIPP, the cornerstone of which is the risk management framework that establishes the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk, and prioritizing CI/KR protection activity. The NIPP provides the unifying structure for the integration of existing and future CI/KR protection efforts into a single national program.

The NIPP delineates roles and responsibilities for security partners in carrying out implementation activities while respecting the authorities, jurisdictions, and prerogatives of these partners. For example, state, territorial, local, and tribal governments are responsible for developing and implementing a CI/KR protection program as a component of their overarching homeland security programs. Regional partners use partnerships that cross jurisdictional and sector boundaries to address CI/KR protection within a defined geographical area. Private sector owners and operators are responsible for undertaking CI/KR protection, coordination, and cooperation activities, as necessary. All of these roles and responsibilities are pertinent to the mission and scope of CGP.

The BZPP offers key support to eligible applicants for nationwide CI/KR protection programs. Federal grants that support CI/KR protection can be grouped into two broad categories: (1) overarching homeland security grant programs that provide funding for a broad set of activities in support of homeland security mission areas and the national priorities outlined in the National Preparedness Goal, and (2) targeted programs for specific threats or CI/KR-related protection initiatives and programs within identified jurisdictions. As required by Congress, infrastructure protection programs include

grants for specific activities that focus on the protection of individual CI/KR sectors, such as ports, mass transit, rail transportation, etc. These funds support CI/KR protection capabilities based on risk and need in coordination with DHS, SSAs, and Federal priorities.

The major goal for this priority in FY 2006 is the successful implementation of the NIPP. The revised NIPP Base Plan will be issued during the Summer of 2006. It will detail milestones and implementation actions to:

- Establish the architecture for conducting risk assessment and risk management activities;
- Provide processes for identifying resource priorities;
- Examine linkages between physical and cyber, domestic and international CI/KR protection efforts;
- Improve information-sharing and public-private-sector coordination; and,
- Integrate steady-state protection programs in an all-hazards environment.

Sector-Specific Plans (SSP) will be delivered to DHS within 180 days of the release of the NIPP Base Plan. Implementing the NIPP and the SSP are important initial steps in achieving and sustaining many of the capabilities identified in the Goal and TCL. The DHS NIPP Program Management Office is responsible for coordinating implementation of the NIPP in partnership with the Sector-Specific Agencies.

Additional information sharing goals DHS will seek to advance with our grant partners during FY 2006 include:

- Build a critical infrastructure protection program that implements the risk management framework outlined in the NIPP. The NIPP will provide more details about the risk management framework and specific approaches to reducing critical infrastructure vulnerability.
- Engage all relevant intergovernmental coordination points (e.g., Federal, state, regional, tribal, local) to ensure a comprehensive approach to critical infrastructure protection across all appropriate levels of government and across both public and private sectors.
- Develop strategies for the protection of CI/KR assets of concern to the region.
- Incorporate cyber security protection efforts across all sectors of CI/KR.

***Important Note*: G&T will continue to update grantees on release of the NIPP Base Plan and associated activities.**

In addition to the overarching priorities, there are four capability-specific priorities. Three are listed here – the fourth, Enhance Medical Surge and Mass Prophylaxis Capabilities, is not relevant to activities associated with these grant programs:

B.4. Strengthen Information Sharing and Collaboration Capabilities

Effective terrorism prevention, protection, response, and recovery efforts depend on timely, accurate information about the identities of the enemies, where they operate, how they are supported, and potential methods of attack. Over the next two years, the Federal government will develop an Information Sharing Environment (ISE) that will enhance existing Federal capabilities and improve linkages with state and local governments.

Major goals for this priority in FY 2006 are:

- Establishing protocols for the routine sharing of threat, vulnerability, and consequence information with DHS through the NOC and Information Sharing and Analysis Centers (ISAC).
- Establishing protocols for receiving and acting on threat information from DHS and other Federal agencies, as well as providing appropriate Federal, state, and local agencies with immediate threat information that may be useful for alerting proper authorities and the public.
- Ensuring that the information fusion process is fully capable of communicating effectively and efficiently with the Federal Government through HSIN, the NOC, the Transportation Security Operations Center (TSOC) and the Department of Transportation's (DOT) Crisis Management Center (CMC), as well as with other intelligence and law enforcement personnel across the Federal Government.
- Utilizing HSIN, which will significantly strengthen the flow of real-time threat information to state, local, and private sector partners at the Sensitive-but-Unclassified level, and provide a platform for communications through the classified SECRET level to state offices.
- Establishing connectivity with the NOC, which will be responsible for taking homeland security-related information and intelligence collected and/or produced via the state fusion process, blending it with up-to-date intelligence collected by Federal entities, and sharing the resulting products with state, tribal, local, and private sector entities via the state's fusion process;
- Integrating and coordinating with key local or regional Federal intelligence entities such as the FBI's Field Intelligence Groups, the Joint Terrorism Task Forces (JTTF), U.S. Immigration and Customs Enforcement's Field Intelligence Units, the U.S. Coast Guard's Field Intelligence Support Teams, the Drug Enforcement Administration's High Intensity Drug Trafficking Area centers and other field intelligence units.

B.5. Strengthen Interoperable Communications Capabilities

The lack of interoperable wireless communication systems is an issue that continues to affect public safety agencies in communities across the country. In many cases, agencies are unable to communicate or share critical voice and data information with other jurisdictions or disciplines during major events or even day-to-day operations. Interoperable communications, a capability-specific priority, is the ability to provide an uninterrupted flow of critical information among responding multi-disciplinary and multi-jurisdictional agencies at all levels of government before, during, and after an event.

Communications interoperability underpins the ability of Federal, state, local, and tribal entities to work together effectively to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies.

The Interoperability Continuum illustrates the five critical elements of success – governance, standard operating procedures, technology, training and exercises, and usage of equipment – that support robust interoperability solutions. These elements include the following activities:

- Governance – A common governing structure for addressing interoperability issues will improve the policies, processes, and procedures of any major project by enhancing communication, coordination, and cooperation; establishing guidelines and principles; and reducing internal jurisdictional conflicts;
- Standard Operating Procedures (SOP) – SOPs are formal written guidelines or instructions for incident response. SOPs typically have both operational and technical components;
- Technology – The technology used to implement interoperable communications is dependent upon existing infrastructure within the region. Multiple technology solutions may be required to support large events;
- Training and Exercises – Proper training and regular exercises are critical to the implementation and maintenance of a successful interoperability solution;
- Usage of Equipment – Usage refers to how often interoperable communication technologies are used.

Major goals for the Communications priority in FY 2006 are:

- Acquisition, implementation, operations, and training on Project 25 standard interoperable digital 2-way wireless communication products and systems, when appropriate.
- Integrating infrastructure communications with state-wide and regional operations plans and procedures to improve public safety and critical infrastructure communications operability and interoperability.
- Training and exercises on public-private partnerships and multi-jurisdictional communications implementation, maintenance, and protocols.
- Establishing public-private assistance or other agreements with surrounding public safety entities in order to effectively maintain or quickly restore emergency communications capabilities and network restoration following a catastrophic event.

B.6. Strengthen Chemical, Biological, Radiological/Nuclear, and Explosive (CBRNE) Detection, Response, and Decontamination Capabilities

This priority seeks to leverage efforts to develop robust capabilities to detect, neutralize, contain, dismantle, and dispose of CBRNE materials, and decontaminate exposed personnel and property. These efforts were heavily emphasized in previous years' G&T grant program guidance.

With specific regard to radiological or nuclear (RAD/NUC) threats, the newly-formed Domestic Nuclear Detection Office (DNDO) plays an essential role in developing and implementing a multi-layered defensive strategy, with domestic and international programs and systems, to protect the Nation from terrorist RAD/NUC attacks. DNDO is working in close coordination with G&T and other Federal, state, local, and tribal entities to develop program guidance that supports the planning, organization, equipment, training, and exercise (POETE) activities related to the enhancement and development of RAD/NUC preventive detection programs at the state and local level. DNDO is also developing operational support systems to assist in the implementation of these programs. State and local grantees are encouraged to work closely with DNDO when developing or enhancing preventive RAD/NUC detection programs in order to ensure compliance with DNDO program guidance and to ensure that state and local programs are effectively integrated into national systems.

Major FY 2006 objectives for the CBRNE Detection priority are as follows:

- Acquisition and deployment of radiological detectors as validated by the DNDO deployment plan.
- Acquisition and deployment of chemical/biological detection systems with a focus on broad system-wide protection for high density, urban transit systems and critical vulnerabilities, specifically infrastructure hubs and nodes.

B.7. Strengthen Emergency Operations Planning and Citizen Protection Capabilities

The devastating aftermath of Hurricane Katrina focused the Nation on the importance of emergency operations planning for catastrophic incidents. As a result, in addition to the National Priorities outlined in the Goal, an additional priority that emphasizes emergency operations and catastrophic planning has been added.

As defined by the NRP, a catastrophic incident is any natural, technical, or man-made incident, including terrorism that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. Catastrophic incidents can result in sustained national impacts over a prolonged period of time; almost immediately exceed resources normally available to State, local, Tribal, and private-sector authorities in the impacted area; and significantly interrupt governmental operations and emergency services to such an extent that national security could be threatened.

As Hurricane Katrina demonstrated, this type of incident affects key planning components including public warning and notification, evacuation, reception and shelter (including a focus on at-risk populations), logistics and resource management, isolation and quarantine, volunteer and donation management, and search and rescue. These factors drive the urgency for coordinated planning to ensure effective initial response and accelerated Federal/national assistance. In November 2005, in response to three discrete tasks from the President and Congress, DHS initiated a national review process of emergency operations plans for all States and 75 Urban Areas. This review is examining the status of catastrophic planning, including mass evacuation planning.

Major goals for the Emergency Operations Planning and Citizen Protection priority in FY 2006 are:

- Establishment of clearly defined and publicly aware evacuation / shelter-in-place plans and protocols that address the unique environment and risks of the infrastructure sector.
- Establish and exercise a means of communicating informative instructions to protect passengers and employees.

APPENDIX G

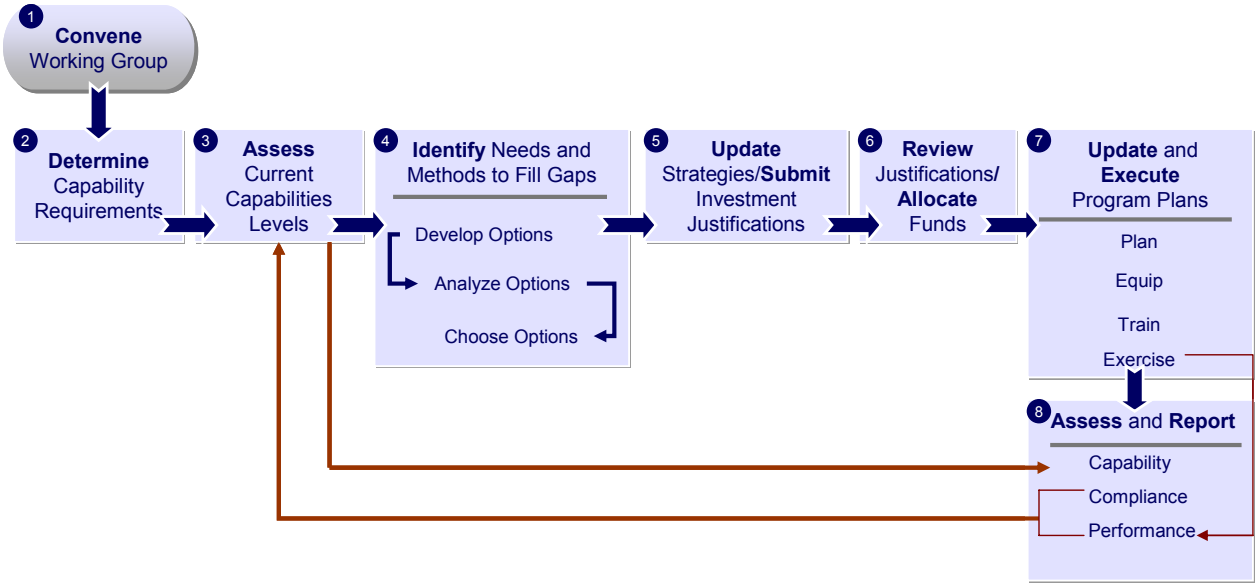
CAPABILITIES BASED PLANNING GUIDANCE

Capabilities Based Planning Guidance

A. Step-by-Step Guide to Capabilities Based Planning

The general process of capabilities based planning is depicted in the figure below. This simple, step-by-step sequence illustrates how process and tools are combined to clearly identify and prioritize requirements, assess current capabilities, and then allocate available resources and emphasis to the most urgently needed capabilities. This description will be refined over time with user feedback and supplemented with specific instructions in annual program guidance.

Figure 4. Capabilities-Based Planning Process



The desired end state is to move the Nation forward to meet the National Preparedness Goal and achieve fully integrated, unified homeland security capabilities. At all levels, information from capabilities-based planning will be used by preparedness programs to refine program structures and strategies. This requires an understanding of needs at the national level through analysis of assessment data. Results of the analyses will be used to update national priorities in the National Preparedness Goal and provide enhanced strategic direction for the Nation.

In conformance with HSPD-8, Federal Departments and Agencies will facilitate the use of a capabilities-based planning process within appropriate homeland security assistance programs. Though specific decision-making processes will vary, they should be able to address similar analytical questions and policy decisions.

APPENDIX H

NATIONAL INCIDENT MANAGEMENT SYSTEM GUIDANCE

National Incident Management System Guidance

A. NIMS Compliance Activities

The NIMS is a comprehensive system that will improve response operations through the use of the Incident Command System (ICS) and other standard procedures and preparedness measures. It will also promote development of cross-jurisdictional, statewide and interstate regional mechanisms for coordinating incident management and obtaining assistance during large-scale or complex incidents.

The NIC recognizes that the overwhelming majority of emergency incidents are handled on a daily basis by a single jurisdiction at the local level. However, it is critically important that all jurisdictions comply with the NIMS because the challenges we face as a Nation are far greater than the capabilities of any one jurisdiction; they are not, however, greater than the sum of all of us working together through mutual support. HSPD- 5, *Management of Domestic Incidents*, requires all Federal Departments and agencies to adopt and implement the NIMS, and requires states, territories, tribes and local governments to implement the NIMS to receive Federal preparedness funding.

States[13] play the integral role in ensuring the effective implementation of the NIMS. They must ensure that the systems and processes are in place to communicate the NIMS requirements to local[14] jurisdictions and support them in implementing the NIMS. The NIMS implementation requirements for local jurisdictions are available in a separate matrix to support this communication and coordination between the states and local jurisdictions. States must also implement specific NIMS implementation actions as outlined in this matrix.

States should encourage and support a regional approach to NIMS implementation among its jurisdictions. In some instances smaller communities may not have the resources to implement all elements of NIMS on their own. However, by working together with other localities in their regions, they will be able to pool their resources to implement NIMS.

When NIMS is fully implemented, states and local jurisdictions will be able to:

---

[13] 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, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States." 6 USC 101 (14)

[14] As defined in the Homeland Security Act of 2002, Section 2(10): the term "local government" means "(A) county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments… regional or interstate government entity, or agency or instrumentality of a local government: an Indian tribe or authorized Tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and a rural community, unincorporated town or village, or other public entity." 6 USC 101(10)

- Ensure common and proven incident management doctrine, practices and principles are used to plan for, protect against, respond to and recover from emergency incidents and preplanned events;
- Maintain a response operation capable of expanding to meet an escalating situation and the ability to integrate resources and equipment from intrastate and interstate mutual aid agreements, state-provided assistance and Federal government response;
- Order and track response assets using common resource typing and definitions, and draw on mutual aid agreements for additional assistance;
- Establish staging and allocation plans for the re-distribution of equipment, supplies and aid coming into the area from other localities, states or the Federal government through mutual aid agreements;
- Conduct situational assessments and establish the appropriate ICS organizational structure to effectively manage the incident;
- Establish communication processes, procedures and protocols that will ensure effective interoperable communications among emergency responders, 911 centers and multi-agency coordination systems such as Emergency Operations Centers (EOC).

How NIMS Applies to CI/KR Sectors:

States should encourage and support a regional approach to NIMS implementation among their homeland security partners, including CI/KR sectors. Further, owners and operators of CI/KR should be well educated on NIMS, as Federal, state, and local responder agencies will utilize its ICS and resource typing in the event of an emergency that impacts their operations or requires their assistance.

For example, the NRP incorporates NIMS as the overarching organizational authority that outlines the roles and responsibilities of the Federal government during an Incident of National Significance. The NRP outlines 15 Emergency Support Functions (ESF) that provide the structure for coordinating Federal interagency support, most of which have direct implications to the Nation's infrastructure:

- ESF 1: Transportation
- ESF 2: Communications
- ESF 3: Public Works and Engineering
- ESF 4: Fire Fighting
- ESF 5: Emergency Management
- ESF 6: Mass Care
- ESF 7: Resource Support
- ESF 8: Health and Medical Services
- ESF 9: Search and Rescue
- ESF 10: Hazardous Materials Response
- ESF 11: Food
- ESF 12: Energy
- ESF 13: Public Safety and Security
- ESF 14: Long-Term Recovery and Mitigation
- ESF 15: External Affairs

In addition, the NRP outlines 10 Support annexes that provide the framework through which Federal departments and agencies, state, local, and tribal entities, the private sector; volunteer organizations and non-governmental organizations coordinate and execute the common functional processes and administrative requirements necessary to ensure efficient and effective incident management.

In order to effectively provide services to assist Federal, state, local and tribal governments in managing an Incident of National Significance, or alternatively, to promptly benefit from response efforts in the event of an emergency, CI/KR owners and operators must be fluent in NIMS.

To prepare for the implementation of NIMS at the Federal, state, and local government levels, owners and operators of CI/KR should:

- Learn the NIMS system, protocols, and terminologies through free, on-line awareness courses provided by DHS;
- Participate in regional homeland security exercises;
- Identify appropriate points of contact and roles within the CI/KR entity to effectively operate with public safety entities in an ICS structure;
- Understand the phased implementation process for states, tribal governments and local jurisdictions to comply with NIMS requirements; and,
- Integrate with existing state/local NIMS implementation strategies, as appropriate.

B. FY 2006 State and Territorial NIMS Compliance Requirements

In Federal Fiscal Year 2005, the Secretary of Homeland Security provided guidance to each state, outlining initial actions that should be taken to implement the NIMS. The letter to the Nation's governors included a list of actions for states and territories to take towards NIMS compliance. A copy of this letter is posted on the NIMS webpage at: http://www.fema.gov/nims/nims_compliance.shtm. Minimum FY 2005 NIMS activities included:

- Incorporating NIMS into existing training programs and exercises;
- Ensuring that Federal preparedness funding (including DHS Homeland Security Grant Program, Urban Area Security Initiative (UASI) funds) support NIMS implementation at the state and local levels (in accordance with the eligibility and allowable uses of the grants);
- Incorporating NIMS into EOPs;
- Promotion of intrastate mutual aid agreements;
- Coordinating and providing technical assistance to local entities regarding NIMS;
- Institutionalizing the use of the ICS.

To receive FY 2006 preparedness grant funds from any Federal Department or agency, states will have to self-certify that they have met the minimum FY 2005 requirements. A self-certification letter will be provided to each state and territory. Additional information is also available on the NIMS Web page at: www.fema.gov/nims.

In Fiscal Year 2006, states, territories, tribes and local communities will be required to complete several activities to comply with the NIMS. The attached implementation matrix describes the actions that states must take by the end of Federal FY 2006 (September 30, 2006) to be compliant with NIMS. These implementation requirements are in addition to the FY 2005 NIMS requirements as established in the Sept. 8, 2004, letter to the governors. A copy of that letter is available on the NIMS Web page at: www.fema.gov/nims.

Beginning in FY 2007, which starts on October 1, 2006, all Federal preparedness funding will be conditioned upon full compliance with the NIMS. By completing the FY 2005 activities as well as the FY 2006 activities outlined in this matrix, states and territories will have achieved what is considered to be full NIMS implementation by FY 2007.

Completion of the FY 2006 actions will result in a statewide infrastructure that will support NIMS implementation among all state and territorial agencies as well as at the tribal and local levels. The effective and consistent implementation of the NIMS in every state and territory will result in a strengthened national capability to prepare for, respond to and recover from any type of incident. The matrix identifies activities that are underway by the NIMS Integration Center to support the effective implementation of NIMS as well as activities that will be required for NIMS implementation in future years.

The matrix also provides information on where to find technical assistance resources to support these compliance actions. For example, the National Incident Management Capability Assessment Support Tool (NIMCAST) is a product designed to assist communities in determining their current NIMS compliance baseline. The NIMS is much more than just a list of required elements; it is a new approach to the way we prepare for and manage incidents, one that will lead to a more effective utilization of resources and enhanced prevention, preparedness and response capabilities. Moreover, full NIMS implementation is a dynamic and multi-year phase-in process with important linkages to the NRP, the Goal and the NIPP. Future refinement to the NIMS will evolve as policy and technical issues are further developed and clarified at the national level. This may well result in additional requirements being issued by the NIC as to what will constitute continuous full NIMS compliance in FY 2007 and beyond.

Table 7. NIMS Implementation Matrix for States and Territories

FY 2006 Compliance Activities		
Required State/Territorial Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
State Adoption and Infrastructure		
Adopt NIMS at the state/ territorial level for all government Departments and agencies; as well as promote and encourage NIMS adoption by associations, utilities, non-governmental organizations (NGOs) and private sector incident management and response organizations. Monitor formal adoption of NIMS by all tribal and local jurisdictions.	• Adopt NIMS through executive order, proclamation, resolution or legislation as the state's official all-hazards, incident response system. • Develop a baseline assessment of NIMS requirements that your jurisdiction already meets and using that baseline, develop a strategy for full NIMS implementation and maintenance. • NIMCAST is available at: www.fema.gov/nimcast/index.jsp • Sample templates for executives: www.fema.gov/nims/nims_toolsandtemplates.shtm	• Amend or re-authorize, as necessary.
Establish a planning process to ensure the communication and implementation of NIMS requirements across the state, including local governments and tribes. This process must provide a means for measuring progress and facilitate reporting.	• FY 2006 NIMS Implementation Matrix for Local Jurisdictions	
Designate a single point of contact within the state government to serve as the principal coordinator for NIMS implementation statewide.	• Consider establishing new or leverage existing cross-jurisdictional and cross-discipline advisory group to assist and ensure full implementation of NIMS.	

FY 2006 Compliance Activities		
Required State/Territorial Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
To the extent permissible by law, ensure that Federal preparedness funding to state and territorial agencies and tribal and local jurisdictions is linked to the satisfactory progress in meeting the requirements related to FY 2006 NIMS implementation requirements.	• *NIM,* March 2004, the NIMS implementation requirements, and Homeland Security Presidential Directive 5 are all available on the NIMS Web page at: www.fema.gov/nims • NIMCAST: www.fema.gov/nimcast/index.jsp • 2005 Homeland Security Grant Program Guidance: http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf • National Preparedness Goal and National Preparedness Guidance: http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm	
To the extent permissible by state and territorial law and regulations, audit agencies and review organizations should routinely include NIMS implementation requirements in all audits associated with Federal preparedness grant funds. This process will validate the self-certification process for NIMS compliance.	• The *National Incident Management System (NIMS)* March 2004, the NIMS implementation requirements, and Homeland Security Presidential Directive 5 are all available on the NIMS Web page at: www.fema.gov/nims • NIMCAST: www.fema.gov/nimcast/index.jsp • A list of the Federal preparedness grant programs that have been reported to the NIC are available on the NIMS Web page at: www.fema.gov/nims • 2005 Homeland Security Grant Program Guidance: http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf • National Preparedness Goal and National Preparedness Guidance: http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm	
Command and Management		
Incident Command System: Manage all emergency incidents and preplanned (recurring/special) events in accordance with ICS organizational structures, doctrine and procedures, as defined in NIMS. ICS implementation must include the consistent application of Incident Action Planning and Common Communications Plans.	• Institutionalize ICS: Terms and definitions: www.fema.gov/txt/nims/institutionalizing_ics.txt • Incorporate concepts and principles of NIMS Chapter II, Command and Management including ICS characteristics such as common terminology, modular organization, management by objectives, incident action planning, manageable span of control, pre-designated incident facilities, comprehensive resource management, integrated communications, transfer of command, unity of command, unified command, personnel and resource accountability and information and intelligence management.	• Continue to manage incidents and events using ICS.

FY 2006 Compliance Activities		
Required State/Territorial Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Multi-agency Coordination System: Coordinate and support emergency incident and event management through the development and use of integrated multi-agency coordination systems, i.e. - develop and maintain connectivity capability between local Incident Command Posts (ICP), local 911 Centers, local EOCs, the state EOC and regional and/Federal EOCs and /NRP organizational elements.	• NIMS Chapter II, Command and Management	• Revise and update processes and plans. • The Emergency Management Institute (EMI) is currently developing an independent study and classroom course on NIMS Multi-Agency Coordination Systems. Additional information will be posted on the NIMS Integration Center Web page when available. See http://www.fema.gov/nims. • The NIMS Integration Center will feature best practices on the NIMS Web page. See http://www.fema.gov/nims.
Public Information System: Institutionalize, within the framework of ICS, the Public Information System, comprising of the Joint Information System (JIS) and a Joint Information Center (JIC). The Public Information System will ensure an organized, integrated, and coordinated mechanism to perform critical emergency information, crisis communications and public affairs functions which is timely, accurate, and consistent. This includes training for designate participants from the Governor's office and key state agencies	• NIMS Chapter II, Command and Management • Public Information Training (E388, Advanced Public Information Officers and G290, Basic Public Information Officers)	• Revise and update processes and plans. • The Emergency Management Institute (EMI) is currently developing an independent study and classroom course on NIMS Public Information Systems. Additional information will be posted on the NIMS Integration Center Web page when available. See http://www.fema.gov/nims. • Information on who should complete these courses also will be posted on the NIMS Web page. • The NIMS Integration Center will feature best practices on the NIMS Web page. See http://www.fema.gov/nims.

FY 2006 Compliance Activities		
Required State/Territorial Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Preparedness: Planning		
Establish the state's NIMS baseline against the FY 2005 and FY 2006 implementation requirements	• Assess which NIMS implementation requirements the state already meets. NIMCAST is available to facilitate this: www.fema.gov/nimcast/index.jsp	• Update state's Homeland Security strategy and any other state preparedness strategies and plans as appropriate and close capability gap.
Coordinate and leverage all Federal preparedness funding to implement the NIMS.	• A list of the Federal preparedness grant programs that have been reported to the NIC are available on the NIMS Web page at: www.fema.gov/nims • 2005 Homeland Security Grant Program Guidance: http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf • National Preparedness Goal and National Preparedness Guidance: http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm • CFDA: http://www.cfda.gov	
Revise and update plans and SOPs to incorporate NIMS and NRP components, principles and policies, to include planning, training, response, exercises, equipment, evaluation and corrective actions	• NRP: http://www.dhs.gov/nationalresponseplan • 2005 Homeland Security Grant Program Guidance: http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf • National Preparedness Goal and National Preparedness Guidance: http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm	• Update plans and SOPs, incorporating lessons learned and best practices from exercises and response operations. • EOP guidance is under development and will be posted on the NIMS Integration Center Web page at: www.fema.gov/nims.

FY 2006 Compliance Activities		
Required State/Territorial Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Promote intrastate and interagency mutual aid agreements, to include agreements with the private sector and non-governmental organizations.	• EMAC model state-county mutual aid deployment contract: http://www.emacweb.org/?123 • EMAC model intrastate mutual aid legislation: http://www.emacweb.org/docs/NEMA%20Proposed%20Intrastate%20Model-Final.pdf	• Expand mutual aid agreements beyond support services and equipment to include information sharing. • Support and adopt the ongoing efforts of the NIC to develop a national credentialing system. • Credentialing guidance is under development by the NIMS Integration Center. Throughout the development process, drafts will be posted on the NIMS Web page for review and comment by interested stakeholders. • Credential first responders in conformance with national standards.
Preparedness: Training		
Leverage training facilities to coordinate and deliver NIMS training requirements in conformance with the NIMS National Standard Curriculum.	• NIMS National Standard Curriculum Training Development Guidance: http://www.fema.gov/pdf/nims/nims_training_development.pdf	

FY 2006 Compliance Activities		
Required State/Territorial Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Complete IS-700 NIMS: An Introduction	• On-line course: http://training.fema.gov/EMIWeb/IS/is700.asp • NIMS National Standard Curriculum Training Development Guidance: http://www.fema.gov/pdf/nims/nims_training_development.pdf • All personnel with a direct role in emergency preparedness, incident management or response must complete this training.	• Ensure that NIMS is part of the program for all new employees, recruits and first responders. • The NIMS Integration Center is working to establish a mechanism that will allow states and local jurisdictions direct access to course completion data. Additional information will be posted on the NIMS Integration Center Web page when available. See http://www.fema.gov/nims.
Complete IS-800 NRP: An Introduction	• On-line course available at: http://www.training.fema.gov/emiweb/IS/is800.asp • NIMS National Standard Curriculum Training Development Guidance: http://www.fema.gov/pdf/nims/nims_training_development.pdf • The NIMS Web page provides guidance for who should complete this training. http://www.fema.gov/nims.	• Ensure that NRP training is part of the program for all appropriate employees, recruits and first responders. • The NIMS Integration Center is working to establish a mechanism that will allow states and local jurisdictions direct access to course completion data. Additional information will be posted on the NIMS Integration Center Web page when available. See http://www.fema.gov/nims.

FY 2006 Compliance Activities		
Required State/Territorial Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Complete ICS 100 and ICS 200 Training	• ICS 100: http://www.training.fema.gov/emiweb/IS/is100.asp • ICS 100: http://www.usfa.fema.gov/training/nfa • ICS 200: http://www.training.fema.gov/emiweb/IS/is200.asp • ICS 200: http://www.usfa.fema.gov/training/nfa • NIMS National Standard Curriculum Training Development Guidance: http://www.fema.gov/pdf/nims/nims_training_development.pdf • The NIMS Web page provides guidance for who should complete this training. http://www.fema.gov/nims.	• Complete ICS 300 and ICS 400. • Complete training that may be required to satisfy credentialing standards. • Ensure that ICS training is part of the program for all new employees, recruits and first responders.
Preparedness: Exercises		
Incorporate NIMS/ICS into all state and regional training and exercises.	• NIMS training information: www.fema.gov/nims/nims_training.shtm • NIMS National Standard Curriculum Training Development Guidance: http://www.fema.gov/pdf/nims/nims_training_development.pdf • DHS G&T Exercise Information: http://www.ojp.usdoj.gov/odp/exercises.htm	• Continue to incorporate NIMS into all state training and exercises, to include drills, tabletop exercises, functional exercises and full-scale exercises.
Participate in an all-hazard exercise program based on NIMS that involves responders from multiple disciplines and multiple jurisdictions.	• 2005 Homeland Security Grant Program Guidance: http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf • National Preparedness Goal and National Preparedness Guidance: http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm • DHS G&T Exercise Information: http://www.ojp.usdoj.gov/odp/exercises.htm • NIMS National Standard Curriculum Training Development Guidance: http://www.fema.gov/pdf/nims/nims_training_development.pdf	• Continue to participate in NIMS -oriented exercises, to include drills, tabletop exercises, functional exercises and full-scale exercises.
Incorporate corrective actions into preparedness and response plans and procedures.	• DHS G&T Exercise Information: http://www.ojp.usdoj.gov/odp/exercises.htm	

FY 2006 Compliance Activities		
Required State/Territorial Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Resource Management		
Inventory state response assets to conform to homeland security resource typing standards.	• Resource typing definitions: http://www.fema.gov/nims/mutual_aid.shtm • Propose modifications or new resource definitions to the NIMS Integration Center for inclusion in the resource typing effort.	• Develop and implement a resource inventory, ordering and tracking system. • The Emergency Management Institute (EMI) is currently developing a course on NIMS Resource Management. Additional information will be posted on the NIMS Integration Center Web page at http://www.fema.gov/nims when the course is available.
Develop state plans for the receipt and distribution of resources as outlined in the NRP Catastrophic Incident Annex and Catastrophic Incident Supplement	• http://www.dhs.gov/nationalresponseplan	
To the extent permissible by state and local law, ensure that relevant national standards and guidance to achieve equipment, communication and data interoperability are incorporated into state and local acquisition programs.	• G&T Equipment Program: http://www.ojp.usdoj.gov/odp/grants_goals.htm • 2005 Homeland Security Grant Program Guidance: http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf • National Preparedness Goal and National Preparedness Guidance: http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm • DHS SAFECOM Program: http://www.safecomprogram.gov/SAFECOM	

FY 2006 Compliance Activities		
Required State/Territorial Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Communication & Information Management		
Apply standardized and consistent terminology, including the establishment of plain English communications standards across public safety sector.	• Incident response communications (during exercises and actual incidents) should feature plain English commands so they will be able to function in a multi-jurisdiction environment. Field manuals and training should be revised to reflect the plain English standard. • '10' codes may continue to be used during non-emergency, internal department communications.	• Continue featuring common terminology and plain English commands for all response activities. • EMI is currently developing an independent study and classroom course on NIMS Communication and Information Management. Additional information will be posted on the NIMS Integration Center Web page when available. See http://www.fema.gov/nims. • Information on who should complete these courses also will be posted on the NIMS Web page.

C. FY 2006 Tribal Government and Local Jurisdiction NIMS Compliance Requirements

In March 2004, the Secretary of Homeland Security, at the request of the President, released the NIMS. The NIMS is a comprehensive system that improves tribal and local response operations through the use of the ICS and the application of standardized procedures and preparedness measures. It promotes development of cross-jurisdictional, statewide, and interstate regional mechanisms for coordinating response and obtaining assistance during a large-scale or complex incident.

Tribal and local authorities, not Federal, have the primary responsibility for preventing, responding to, and recovering from emergencies and disasters. The overwhelming majority of emergency incidents are handled on a daily basis by a single jurisdiction at the local level. It is critically important that all jurisdictions comply with the NIMS because the challenges we face as a Nation are far greater than the capabilities of any one jurisdiction; they are not, however, greater than the sum of all of us working together through mutual support. HSPD-5, *Management of Domestic Incidents*,

requires all Federal Departments and agencies to adopt and implement the NIMS, and requires state[15] and local[16] jurisdictions to implement the NIMS to receive Federal preparedness funding.

NIMS compliance should be considered and undertaken as a community-wide effort. The benefit of NIMS is most evident at the local level, when a community as a whole prepares for and provides an integrated response to an incident. Incident response organizations (to include local public health, public works, emergency management, fire, emergency medical services, law enforcement, hazardous materials, private sector entities, non-governmental organizations, medical organizations, utilities, and others) must work together to comply with NIMS components, policies, and procedures. Implementation of the NIMS in every tribal and local jurisdiction establishes a baseline capability that once established nationwide, can be used as a foundation upon which more advanced homeland security capabilities can be built.

Small and/or rural jurisdictions will benefit from a regional approach. In many instances smaller communities may not have the resources to implement all elements of NIMS on their own. However, by working together with other localities in their regions, these jurisdictions will be able to pool their resources to implement NIMS.

When NIMS is fully implemented, your Tribal or local jurisdiction will be able to:

- Ensure common and proven incident management doctrine, practices, and principles are used to plan for, protect against, respond to, and recover from emergency incidents and preplanned events;
- Maintain a response operation capable of expanding to meet an escalating situation and the ability to integrate resources and equipment from intrastate and interstate mutual aid agreements, state-provided assistance, and Federal government response;
- Order and track response assets using common resource typing and definitions, and draw on mutual aid agreements for additional assistance;
- Establish staging and allocation plans for the re-distribution of equipment, supplies, and aid coming into the area from other localities, states, or the Federal government through mutual aid agreements;
- Conduct situational assessments and establish the appropriate ICS organizational structure to effectively manage the incident; and
- Establish communication processes, procedures and protocols that will ensure effective interoperable communications among emergency responders, 911 centers, and multi-agency coordination systems (EOCs).

[15] 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, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States." 6 USC 101 (14)

[16] As defined in the Homeland Security Act of 2002, Section 2(10): the term "local government" means "(A) county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments… regional or interstate government entity, or agency or instrumentality of a local government: an Indian tribe or authorized Tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and a rural community, unincorporated town or village, or other public entity." 6 USC 101(10)

In Federal Fiscal Year 2005, the Secretary of Homeland Security provided guidance to each state, outlining initial actions that should be taken to implement the NIMS. The letter to the Nation's governors included a list of recommended actions for tribal and local governments to help them work towards NIMS compliance. A copy of this letter is posted on the NIMS webpage at: http://www.fema.gov/nims/nims_compliance.shtm. Recommended FY 2005 NIMS activities included:

- Institutionalize the use of the Incident Command System;
- Complete the NIMS awareness course IS-700 NIMS: An Introduction;
- Formally recognize NIMS and adopt NIMS principles and policies;
- Establish a NIMS compliance baseline by determining the NIMS requirements that have already been met; and
- Develop a strategy and timeline for full NIMS implementation.

By completing these activities, communities will have made substantial progress toward full NIMS implementation by the start of Fiscal Year 2007 (i.e. October 1, 2006). In Federal Fiscal Year 2006, tribes and local communities will be required to complete several activities to comply with the NIMS. The following implementation matrix describes the actions that jurisdictions must take by September 30, 2006 to be compliant with NIMS.

Completion of these actions will position tribal and local communities to better manage prevention, response and recovery efforts. The matrix identifies activities that are underway by the NIC to support the effective implementation of NIMS as well as activities that will be required for NIMS implementation in future years.

The matrix also provides information on where to find technical assistance resources to support these compliance actions. For example, NIMCAST is an example of a product designed to assist communities in determining their current NIMS compliance baseline. The NIMS is much more than just a list of required elements; it is a new approach to the way we prepare for and manage incidents, one that will lead to a more effective utilization of resources and enhanced prevention, preparedness, and response capabilities. Moreover, full NIMS implementation is a dynamic and multi-year phase-in process with important linkages to the NRP, the HSPD-8 (i.e. the "National Preparedness Goal") and the NIPP. Future refinement to the NIMS will evolve as policy and technical issues are further developed and clarified at the national level. This may well result in additional requirements being issued by the NIC as to what will constitute continuous full NIMS compliance in FY 2007 and beyond.

Table 8. NIMS Implementation Matrix for Tribal and Local Jurisdictions

FY 2006 Compliance Activities		
Required Tribal/Local Jurisdiction Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Community Adoption		
Adopt NIMS at the community level for all government Departments and agencies; as well as promote and encourage NIMS adoption by associations, utilities, non-governmental organizations (NGOs), and private sector incident management and response organizations.	• Adopt NIMS through executive order, proclamation, resolution, or legislation as the jurisdiction's official all-hazards, incident response system. • Develop a baseline assessment of the NIMS implementation requirements that your jurisdiction already meets and using that baseline, develop a strategy for full NIMS implementation and maintenance. • NIMCAST is available at: www.fema.gov/nimcast/index.jsp • Sample templates for executives: www.fema.gov/nims/nims_toolsandtemplates.shtm	• Amend or re-authorize, as necessary.
Command and Management		
Incident Command System (ICS): Manage all emergency incidents and preplanned (recurring/special) events in accordance with ICS organizational structures, doctrine, and procedures, as defined in NIMS. ICS implementation must include the consistent application of Incident Action Planning and Common Communications Plans.	• Institutionalize ICS: Terms and definitions: www.fema.gov/txt/nims/institutionalizing_ics.txt • Incorporate concepts and principles of NIMS Chapter II, Command and Management including ICS characteristics such as common terminology, modular organization, management by objectives, incident action planning, manageable span of control, pre-designated incident facilities, comprehensive resource management, integrated communications, transfer of command, unity of command, unified command, personnel and resource accountability, and information and intelligence management.	• Continue to manage incidents and events using ICS.

FY 2006 Compliance Activities		
Required Tribal/Local Jurisdiction Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Multi-agency Coordination System: Coordinate and support emergency incident and event management through the development and use of integrated multi-agency coordination systems, i.e. develop and maintain connectivity capability between local Incident Command Posts (ICPs, local 911 Centers, local Emergency Operations Centers (EOCs) and state EOC.	• NIMS Chapter II, Command and Management	• Revise and update processes and plans. • The Emergency Management Institute (EMI) is currently developing an independent study and classroom course on NIMS Multi-Agency Coordination Systems. Additional information will be posted on the NIMS Integration Center Web page when available. See http://www.fema.gov/nims. • The NIMS Integration Center will feature best practices on the NIMS Web page. See http://www.fema.gov/nims.
Public Information System: Implement processes, procedures, and/or plans to communicate timely, accurate information to the public during an incident through a Joint Information System and Joint Information Center.	• NIMS Chapter II, Command and Management • Public Information Training (E388, Advanced Public Information Officers and G290, Basic Public Information Officers)	• Revise and update processes and plans. • The Emergency Management Institute (EMI) is currently developing an independent study and classroom course on NIMS Public Information Systems. Additional information will be posted on the NIMS Integration Center Web page when available. See http://www.fema.gov/nims. • Information on who should complete these courses also will be posted on the NIMS Web page. • The NIC will feature best practices on the NIMS Web page. See http://www.fema.gov/nims.
Preparedness: Planning		
Establish the community's NIMS baseline against the FY 2005 and FY 2006 implementation requirements.	• Assess which NIMS implementation requirements your community already meets. NIMCAST is available to facilitate this: www.fema.gov/nimcast/index.jsp	• Update strategy as appropriate and close capability gap.

FY 2006 Compliance Activities		
Required Tribal/Local Jurisdiction Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Develop and implement a system to coordinate all Federal preparedness funding to implement the NIMS across the community.	• A list of the Federal preparedness grant programs that have been reported to the NIC are available on the NIMS Web page at: www.fema.gov/nims • 2005 Homeland Security Grant Program Guidance: http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf • National Preparedness Goal and National Preparedness Guidance: http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm • Catalog of Federal Domestic Preparedness Assistance (CFDA): http://www.cfda.gov	
Revise and update plans and SOPs to incorporate NIMS components, principles and policies, to include planning, training, response, exercises, equipment, evaluation, and corrective actions	• 2005 Homeland Security Grant Program Guidance: http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf • National Preparedness Goal and National Preparedness Guidance: http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm	• Update plans and SOPs, incorporating lessons learned and best practices from exercises and response operations. • Emergency Operations Plan (EOP) guidance is under development and will be posted on the NIMS Integration Center Web page at: www.fema.gov/nims.
Participate in and promote intrastate and interagency mutual aid agreements, to include agreements with the private sector and non-governmental organizations.	• EMAC model state-county mutual aid deployment contract: http://www.emacweb.org/?123 • EMAC model intrastate mutual aid legislation: http://www.emacweb.org/docs/NEMA%20Proposed%20Intrastate%20Model-Final.pdf	• Expand mutual aid agreements beyond support services and equipment to include information sharing. • Support and adopt the ongoing efforts of the NIC to develop a national credentialing system. • Credentialing guidance is under development by the NIMS Integration Center. Throughout the development process, drafts will be posted on the NIMS Web page for review and comment by interested stakeholders. • Credential first responders in conformance with national standards.

FY 2006 Compliance Activities		
Required Tribal/Local Jurisdiction Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Preparedness: Training		
Complete IS-700 NIMS: An Introduction	• On-line course: http://training.fema.gov/EMIWeb/IS/is700.asp • NIMS National Standard Curriculum Training Development Guidance: http://www.fema.gov/pdf/nims/nims_training_development.pdf • All personnel with a direct role in emergency preparedness, incident management, or response must complete this training	• Ensure that NIMS training is part of the program for all new employees, recruits and first responders who have a direct role in emergency preparedness, incident management, or response. • The NIMS Integration Center is working to establish a mechanism that will allow state and local jurisdictions direct access to course completion data. Additional information will be posted on the NIMS Integration Center Web page when available. See http://www.fema.gov/nims.
Complete IS-800 NRP: An Introduction	• On-line course available at: http://www.training.fema.gov/emiweb/IS/is800.asp • NIMS National Standard Curriculum Training Development Guidance: http://www.fema.gov/pdf/nims/nims_training_development.pdf • The NIMS Web page provides for who should complete this training. http://www.fema.gov/nims	• Ensure that NRP training is part of the program for all appropriate new employees, recruits and first responders. • The NIMS Integration Center is working to establish a mechanism that will allow state and local jurisdictions direct access to course completion data. Additional information will be posted on the NIMS Integration Center Web page when available. See http://www.fema.gov/nims.

FY 2006 Compliance Activities		
Required Tribal/Local Jurisdiction Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Complete ICS 100 and ICS 200 Training	• ICS 100: http://www.training.fema.gov/emiweb/IS/is100.asp • ICS 100: http://www.usfa.fema.gov/training/nfa • ICS 200: http://www.training.fema.gov/emiweb/IS/is200.asp • ICS 200: http://www.usfa.fema.gov/training/nfa • NIMS National Standard Curriculum Training Development Guidance: http://www.fema.gov/pdf/nims/nims_training_development.pdf • The NIMS Web page provides guidance for who should complete this training. http://www.fema.gov/nims.	• Complete ICS 300 and ICS 400. • Complete training that may be required to satisfy credentialing standards. • Ensure that ICS training is part of the program for all new employees, recruits and first responders. • The NIMS Integration Center is working to establish a mechanism that will allow states and local jurisdictions direct access to course completion data. Additional information will be posted on the NIMS Integration Center Web page when available. See http://www.fema.gov/nims.
Preparedness: Exercises		
Incorporate NIMS/ICS into all tribal, local and regional training and exercises.	• NIMS training information: http://www.fema.gov/nims/nims_training.shtm • NIMS National Standard Curriculum Training Development Guidance: http://www.fema.gov/pdf/nims/nims_training_development.pdf • DHS G&T Exercise Information: http://www.ojp.usdoj.gov/odp/exercises.htm	• Continue to incorporate NIMS into all local training and exercises, to include drills, tabletop exercises, functional exercises, and full-scale exercises.
Participate in an all-hazard exercise program based on NIMS that involves responders from multiple disciplines and multiple jurisdictions.	• 2005 Homeland Security Grant Program Guidance: http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf • National Preparedness Goal and National Preparedness Guidance: http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm • DHS G&T Exercise Information: http://www.ojp.usdoj.gov/odp/exercises.htm • NIMS National Standard Curriculum Training Development Guidance: http://www.fema.gov/pdf/nims/nims_training_development.pdf	• Continue to participate in NIMS -oriented exercises, to include drills, tabletop exercises, functional exercises, and full-scale exercises.

FY 2006 Compliance Activities		
Required Tribal/Local Jurisdiction Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Incorporate corrective actions into preparedness and response plans and procedures.	• DHS G&T Exercise Information: http://www.ojp.usdoj.gov/odp/exercises.htm	
Resource Management		
Inventory community response assets to conform to homeland security resource typing standards.	• Propose modifications or new resource definitions to the NIMS Integration Center for inclusion in the resource typing effort. • Resource typing definitions: http://www.fema.gov/nims/mutual_aid.shtm	• Develop and implement a resource inventory, ordering, and tracking system. • The Emergency Management Institute (EMI) is currently developing a course on NIMS Resource Management. Additional information will be posted on the NIMS Integration Center Web page at http://www.fema.gov/nims when the course is available.
To the extent permissible by law, ensure that relevant national standards and guidance to achieve equipment, communication, and data interoperability are incorporated into tribal and local acquisition programs.	• G&T Equipment Program: http://www.ojp.usdoj.gov/odp/grants_goals.htm • 2005 Homeland Security Grant Program Guidance: http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf • National Preparedness Goal and National Preparedness Guidance: http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm • DHS SAFECOM Program: http://www.safecomprogram.gov/SAFECOM	

FY 2006 Compliance Activities		
Required Tribal/Local Jurisdiction Action for FY 2006 Compliance	**Guidance and Technical Assistance Resources**	**Future Activities**
Communication & Information Management		
Apply standardized and consistent terminology, including the establishment of plain English communications standards across public safety sector.	• Incident response communications (during exercises and actual incidents) should feature plain English commands so they will be able to function in a multi-jurisdiction environment. Field manuals and training should be revised to reflect the plain English standard. • '10' codes may continue to be used during non-emergency, internal Department communications.	• Continue featuring common terminology and plain English commands for all response activities. • The Emergency Management Institute (EMI) is currently developing a course on NIMS Communication and Information Management. Additional information will be posted on the NIMS Integration Center Web page at http://www.fema.gov/nims when the course is available.

***Important Note*: Additional information on NIMS, NIMS compliance and answers to frequently asked questions are available on the NIMS Integration Center Web page (*http://www.fema.gov/nims*).**

APPENDIX I

NATIONAL INFRASTRUCTURE PROTECTION PLAN GUIDANCE

National Infrastructure Protection Plan

The overarching goal of the NIPP is to:

> *Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and enabling national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.*

Achieving this goal requires meeting a series of objectives that include: understanding and sharing information about terrorist threats and other hazards, building security partnerships, implementing a long-term risk-management program and maximizing the efficient use of resources. Measuring progress toward achieving the NIPP goal requires that CI/KR security partners have:

- Coordinated risk-based CI/KR plans and programs in place addressing known and foreseeable threats and hazards;
- Structures and processes that are flexible and adaptable both to incorporate lessons learned and best practices and also to quickly adapt to a changing threat or incident environment;
- Processes in place to identify and address dependencies and interdependencies to allow for more timely and effective implementation of short-term protective actions and more rapid response and recovery; and
- Access to robust information-sharing networks that include relevant intelligence and threat analysis and real-time incident reporting.

A. The NIPP Value Proposition

The public-private partnership called for in the NIPP provides the foundation for effective CI/KR protection. Government and private sector partners bring core competencies that add value to the partnership. Prevention, protection, response and recovery efforts are most efficient and effective when there is full participation at all levels of government and with industry partners.

The success of the partnership depends on articulating the mutual benefits to government and private sector partners. While the value proposition to the government is clear, it is often more difficult to articulate the direct benefits to participation for the private sector. Industry provides the following capabilities, outside of government core competencies:

- Ownership and management of a vast majority of critical infrastructures in most sectors;
- Visibility into CI/KR assets, networks, facilities, functions, and other capabilities;
- Ability to take actions as first responders to incidents;
- Ability to innovate and to provide products, services, and technologies to quickly focus on requirements; and

- Existing, robust mechanisms useful for sharing and protecting sensitive information on threats, vulnerabilities, countermeasures, and best practices.

In assessing the value proposition for the private sector, there is a clear national security and homeland security interest in ensuring the protection of the Nation's CI/KR. Government can encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad-scale infrastructure protection through activities such as:

- Providing owners and operators timely, analytical, accurate, and useful information on threats to CI/KR;
- Ensuring industry is engaged, as early as possible in the development of initiatives and policies related to the implementation and, as needed, revision of the NIPP base plan;
- Ensuring industry is engaged, as early as possible the development and revision of the Sector-Specific Plans (SSPs) and in planning and other CI/KR protection initiatives;
- Articulating to corporate leaders, through the use of public platforms and private communications, both the business and national security benefits of investing in security measures that exceed their business case;
- Creating an environment that encourages and supports incentives for companies to voluntarily adopt widely accepted, sound security practices;
- Working with industry to develop and clearly prioritize key missions and enable their protection or restoration;
- Providing support for research needed to enhance future CI/KR protection efforts;
- Developing the resources to engage in cross-sector interdependency studies, through exercises and computer modeling, that result in guided decision support for business continuity planning; and
- Enabling time-sensitive restoration and recovery support to priority CI/KR facilities and services during incidents in accordance with provisions of the Robert T. Stafford Disaster Relief and Emergency Assistance Act and the NRP.

B. Risk Management Framework

The above examples illustrate some of the ways in which the government can, by actively partnering with the private sector, add value to industry's ability to assess its own risk and refine its business continuity plans, as well as contribute to the security and economic vitality of the Nation. The NIPP outlines the high-level value in the overall public-private partnership for CI/KR protection. The SSPs will outline specific future activities and initiatives that articulate the corresponding valued to those sector-specific CI/KR partnerships and protection activities.

The cornerstone of the NIPP is its risk management framework. Risk, in the context of the NIPP, is defined as the potential for loss, damage or disruption to the Nation's CI/KR resulting from destruction, incapacitation or exploitation during some future man-made or naturally occurring event. The NIPP risk management framework establishes the process for combining consequence, vulnerability and threat information to produce a

comprehensive, systematic and rational assessment of national or sector-specific risk that drives prioritized CI/KR-protection activities. The framework applies to the general threat environment, as well as to specific threats or incident situations. The NIPP risk management framework includes the following activities:

- **Set security goals:** Define specific outcomes, conditions, end points or performance targets that collectively constitute an effective protective posture.

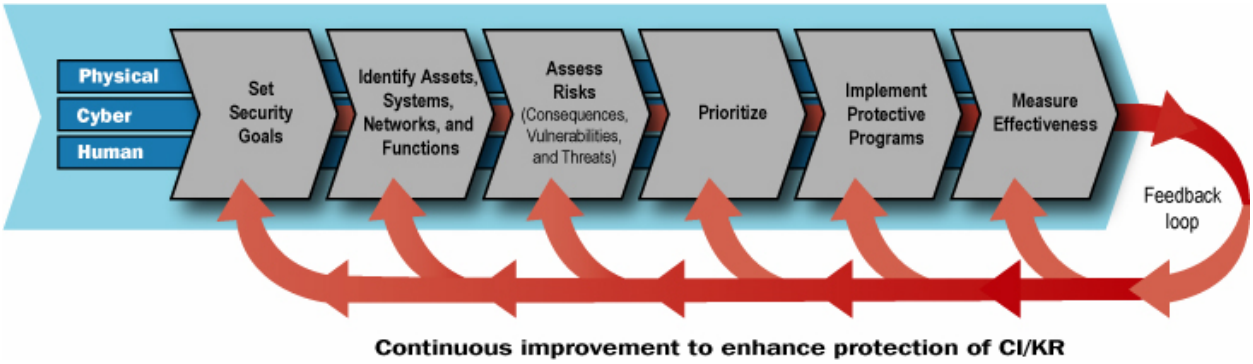
- **Identify assets, systems, networks, and functions:** Develop an inventory of the assets, systems, and networks, including those located outside the United States, that compose the Nation's infrastructure and the critical functionality therein; collect information pertinent to risk management that takes into account the fundamental characteristics of each sector.

- **Assess risks:** Determine risk by combining potential direct and indirect consequences of a terrorist attack or other hazards (including seasonal changes in consequences, dependencies and interdependencies associated with each identified asset, system, or network), known vulnerabilities to various potential attack vectors, and general or specific threat information.

- **Prioritize:** Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk; establish priorities based on risk and determine protection and business continuity initiatives that provide the greatest reduction in risk for the allocation of resources.

- **Implement protective programs:** Select sector-appropriate protective actions or programs to reduce or manage the risk identified; secure the resources needed to address priorities.

- **Measure effectiveness:** Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national CI/KR protection program in improving protection, reducing risk, and increasing resiliency.



The NIPP provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort that brings together government at all levels, the private sector and international organizations and allies. In addition, the SSPs mandated by the NIPP detail the application of the NIPP framework

to each CI/KR sector. SSPs are developed by the designated Federal SSAs in coordination with sector security partners. Together, these plans provide the mechanisms for identifying assets, systems and networks; understanding threats, assessing vulnerabilities and consequences; prioritizing protection initiatives and investments based on costs and benefits so that they are used where they offer the greatest reduction of risk; and, implementing information-sharing and protection measures within and across CI/KR sectors.

The NIPP also delineates the roles and responsibilities for carrying out these activities while respecting the authorities, jurisdictions and prerogatives of the various public and private sector security partners involved. Implementing the NIPP will involve the integrated and coordinated support of all security partners with infrastructure protection responsibilities across the country and internationally.

The NIPP covers the full range of CI/KR sectors as defined in HSPD-7. The framework is applicable to all security partners with CI/KR protection responsibilities and includes explicit roles and responsibilities for the Federal government, including CI/KR under the control of the legislative, executive or judicial branches. Federal departments and agencies with specific responsibilities for CI/KR protection are required to take actions in accordance with the NIPP. The NIPP also provides an organizational structure, protection guidelines and recommended activities for other security partners to help ensure consistent implementation of the national framework and the most effective use of resources.

C. Example: Leveraging Resources to Support Homeland Security and CI/KR Protection Activities of a Mass Transit System

The following example provides an illustration of how the various funding sources described in this chapter can work together in a practical situation to address the CI/KR protection needs of a local system that, through implementation of the NIPP Risk Management Framework and SSP processes, is deemed to be critical to the Nation. This example focuses on a mass transit system in a community that participates in the UASI program. In this situation, the following resources may be applied to support the safety and security of the mass transit system:

Owner Operator Responsibilities
The local mass transit authority, as the owner and operator of the system, funds system-specific protection and security measures including resiliency and business continuity planning activities for the system on a day-to-day basis.

State, Local, and Tribal Government Responsibilities
The State and local governments supports the day-to-day protection of the public; enforce security, protective and preventive measures around the system's facilities; and, provide response and/or recovery capabilities should an incident occur.

Federal Support and Grant Funding
Assistance from the Federal Government through variety of resources, including grants (both Targeted Infrastructure Protection Programs and overarching homeland security

grant programs), training, technical assistance and exercises, further support and enhance ongoing homeland security and CI/KR protection activities. In this example, DHS (as the SSA for the Transportation Sector) and the Department of Transportation (DOT) may contribute to the protection efforts through either appropriated program funds or grants. The range of grants that, based on eligibility, may support of the overall protection of this system includes:

- If the mass transit system is eligible for infrastructure protection program funding, such as the **FY 2006 TSGP**, this funding source may be leveraged to support security enhancements for the mass transit system.
- If the mass transit system is eligible under the **BZPP**, this funding source may also be leveraged to improve security around the system or enhance preparedness capabilities within the surrounding community.
- **Homeland Security Grant Program** funding from programs such as **State Homeland Security Program, Urban Areas Security Initiative, and Law Enforcement Terrorism Prevention Program**, may be leveraged to enhance prevention, protection, response, and recovery capabilities in and around the mass transit system, if the system is deemed critical by the state and/or local authorities within their homeland security strategies and priorities, and in accordance with allowable cost guidance.
- **The Assistance to Firefighters Grant (AFG)** program may be leveraged to support preparedness capabilities of the local fire department that are necessary to protect the system within the city.
- DOT's **Federal Transit Administration** grant programs to support metropolitan and state planning may be leveraged to provide planning for upgrades to the system which include more resilient CI/KR design, and the major capital investments and special flexible funding grant programs may be leveraged to help build these improvements.

All of these resources, used in support of the region's mass transit system, are coordinated with State and Urban Area homeland security strategies, as well as the applicable RTSS. Additionally, other services, training, exercises, and/or technical assistance (for example, the DHS/G&T Mass Transit Technical Assistance Program, which includes a facilitated risk assessment) may be leveraged from a variety of Federal partners.

APPENDIX J

DOMESTIC NUCLEAR DETECTION OFFICE GUIDANCE

Domestic Nuclear Detection Office Guidance

A. Mission and Vision

As part of the national effort to protect the Nation from radiological and nuclear threats, the Domestic Nuclear Detection Office (DNDO) was established by Presidential Directive on April 15, 2005. The DNDO is now the primary agency within the U.S. Government responsible for developing the Global Nuclear Detection Architecture, and acquiring and supporting the deployment of the domestic detection system to detect and report attempts to import or transport a nuclear device or fissile or radiological material, intended for illicit use. The Director of DNDO reports to the Secretary, DHS.

Among these program initiatives, DNDO is conducting both evolutionary (near-term requirements-driven) and transformational (long-term, high pay-off) research, development, test, and evaluation (RDT&E) programs to improve the Nation's capabilities for detection, identification, and reporting of radiological and nuclear materials. By integrating these RDT&E programs with operational support responsibilities, the DNDO will ensure that all technologies will be appropriately deployed, with training materials and well-developed operational response protocols, and that systems that are fielded are complementary and not duplicative, so that the resources and components comprising the global architecture are maximally effective.

DNDO plays an essential role in creating and implementing a multi-layered defensive strategy, with domestic and international programs, to protect the Nation from a terrorist nuclear or radiological attack. No single layer within the strategy will be capable of providing one hundred percent effectiveness in detecting and interdicting nuclear materials intended for illicit use.

B. Critical Infrastructure Partnerships

G&T recognizes the important contribution that effective sharing and use of nuclear detection-related information, intelligence, and systems play in strengthening our Nation's security posture. DNDO will integrate crucial overseas detection programs with domestic nuclear detection systems and other nuclear detection efforts undertaken by Federal, state, local, and tribal governments and private sector. To facilitate an effective engagement with owners and operators of CI/KR that are involved in RAD/NUC preventive detection activities, DNDO is developing a database of entities pursuing preventive detection programs and will engage with them in the incremental deployment of a layered defense strategy.

C. Allowable Costs

DNDO encourages states and regions to implement a comprehensive nuclear detection program capable of detecting nuclear weapons and radiological dispersal devices in support of and in concert with the national global nuclear detection architecture. DNDO believes that implementation of a comprehensive program will take several years, and will require substantial interstate and Federal coordination. As such, DNDO intends, to the extent possible, to partner with state, local, and tribal agencies, as well as the private sector choosing to implement nuclear detection systems with regard to architecture design, subsystem configuration, upgrades and coordinated operations, communications and interoperability.

DNDO believes that an initial layer of detection may include fixed and mobile radiation portal monitors, handheld and other mobile nuclear detection devices as well as radiography systems.

Funding from the BZPP can be used to enhance existing or establish new preventive RAD/NUC detection programs. However, grantees must contact DNDO prior to initiating program activities and provide a point of contact for each detection program to whom DNDO can provide program guidance and updates. Please contact DNDO with this information at DNDO.SLA@hq.dhs.gov.

D. Establishing and Enhancing Programs

DNDO is working in close coordination with G&T and other Federal, state, and local entities to develop technical assistance (TA) programs for the enhancement and development of RAD/NUC preventive detection programs that support planning, organization, equipment, training, and exercises activities (POETE). This POETE framework matches to the Goal, RTSS and all reporting requirements for G&T grant programs. DNDO is also developing operational support systems to assist in the implementation of these programs.

In FY 2006, TA will include making equipment test results available on the Responder Knowledge Base (RKB) to inform stakeholder's procurement decisions. Additionally, in FY 2006 DNDO anticipates publishing guidance for establishing response protocols; guidance on linking programs to state fusion centers; and guidance on utilizing operational support systems. The table below provides an overview of the types of guidance and support systems that DNDO will develop.

An example of detection enhancement that DNDO specifically supports and endorses is commercial vehicle inspection (CVI) related programs. CVI programs should consist of both fixed and mobile systems, and will tie into DNDO's global and domestic nuclear detection reporting system. By the end of 2006, DNDO anticipates developing program guidance and operational support mechanisms specifically related to commercial vehicle inspection, to include guidance on protocols, equipment procurement, training, and exercises that can be customized for specific state/regional programs. Grant applicants are encouraged to consider developing or enhancing detection capabilities in

this area, and to work closely with DNDO in that process. In addition to the CVI program, DNDO is developing program guidance for the employment of mobile and human portable detection equipment to enhance static detection programs such as CVI. These programs will be focused on providing standardization in flexible detection resources and, like CVI, will include guidance on protocols, equipment procurement, training and exercises.

In all cases where grant applicants are developing or enhancing preventive detection capabilities, it is important to link those systems into DNDO's domestic and global detection reporting system. The architecture is being designed to provide 24/7 global awareness on RAD/NUC issues (shipments, alerts, etc.) and provide technical operational support (reachback) for detection alarm resolution. Information about DNDO's operational support and other programs can be obtained by contacting DNDO at the e-mail address noted above.

Table 9. TA for RAD/NUC Preventive Detection Programs

Planning	DNDO will provide assistance with planning and development of protocols and programs.
Organization	DNDO will provide guidance for organizational structures to support successful RAD/NUC preventive detection programs.
Equipment	DNDO will identify equipment and integrated layers of equipment to meet detection and response mission priorities.
Training	DNDO will help develop and implement training and training guidelines.
Exercises	DNDO will provide assistance with enhancing and developing exercise guidelines and support.
Operational Support	DNDO is establishing technical reachback support systems and other 24/7 information sharing systems

Grantees are encouraged to work closely with DNDO as they develop preventive RAD/NUC detection programs in order to ensure compliance with DNDO program guidance and to ensure that national operational support systems are effectively integrated into their programs.

APPENDIX K

ACRONYMS AND ABBREVIATIONS

Acronyms and Abbreviations

A

AAR	After Action Reports
ACH	Automated Clearing House
AEL	Authorized Equipment List
ASAP	Automated Standard Application for Payments

B

BSIR	Biannual Strategy Implementation Reports
BZP	Buffer Zone Plan
BZPP	Buffer Zone Protection Program

C

CAPR	Categorical Assistance Progress Reports
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CCP	Citizen Corps Program
CCTV	Closed-Circuit Television
CFR	Code of Federal Regulations
CFDA	Catalog of Federal Domestic Assistance
CI/KR	Critical Infrastructure/Key Resources
CIP	Critical Infrastructure Protection
CMIA	Cash Management Improvement Act
CSID	Centralized Scheduling and Information Desk
CWIN	Critical Infrastructure Warning Network

D

D&B	Dun and Bradstreet
DHS	U.S. Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DOJ	U.S. Department of Justice
DOT	U.S. Department of Transportation
DPETAP	Domestic Preparedness Equipment Technical Assistance Program
DUNS	Data Universal Numbering System

E

EA	Environmental Assessment
EIS	Environmental Impact Statement
EMPG	Emergency Management Performance Grants
EMS	Emergency Medical Services
EOP	Emergency Operations Plan
EPA	U.S. Environmental Protection Agency

F

FAR	Federal Acquisition Regulations
FBI	Federal Bureau of Investigation
FICA	Federal Insurance Contributions Act
FOIA	Freedom of Information Act
FSR	Financial Status Report

G

G&T	Preparedness Directorate's Office of Grants and Training
GAN	Grant Adjustment Notice
GMS	Grants Management System

H

HAZMAT	Hazardous Materials
HDER	Homeland Defense Equipment Reuse
HHS	U.S. Department of Health and Human Services
HSA	Homeland Security Advisor
HSGP	Homeland Security Grant Program
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
HSPTAP	Homeland Security Preparedness Technical Assistance Program
HSVAC	Homeland Security Virtual Assistance Center

I

IAB	InterAgency Board
IAFIS	Integrated Automated Fingerprint Identification System
IBSGP	Intercity Bus Security Grant Program
IP	Office of Infrastructure Protection
IPRSGP	Intercity Passenger Rail Security Grant Program

J

JRIES	Joint Regional Information Exchange System
JTTF	Joint Terrorism Task Force

L

LEP	Limited English Proficient
LETPP	Law Enforcement Terrorism Prevention Program
LLIS	Lessons Learned Information Sharing
LOCES	Letter of Credit Electronic Certification System

M

M&A	Management and Administrative
MIPT	National Memorial Institute for the Prevention of Terrorism
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MMRS	Metropolitan Medical Response System

N

NCIC	National Crime Information Center
NEPA	National Environmental Policy Act
NGO	Non-Governmental Organization
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NOC	National Operations Center
NRP	National Response Plan
NSSE	National Special Security Event

O

OC	Office of the Comptroller
OI&A	Office of Intelligence and Analysis
OJP	Office of Justice Programs
OGO	Office of Grant Operations
OMB	Office of Management and Budget

P

PAPRS	Phone Activated Paperless Request System
PCII	Protected Critical Infrastructure Information
POC	Point of Contact
PSA	Protective Security Advisor
PSGP	Port Security Grant Program

R

RAD/NUC	Radiological and Nuclear
RKB	Responder Knowledge Base
RMD	Risk Management Division
RTSWG	Region Transit Security Working Group

S

SAA	State Administrative Agency
SEL	Standardized Equipment List
SHSP	State Homeland Security Program
SME	Subject Matter Expert
SOP	Standard Operating Procedure
SPOC	Single Point of Contact
SSA	Sector Specific Agency
SSP	Sector Specific Plan

T

TA	Technical Assistance
TCL	Target Capabilities List
TSA	Transportation Security Administration
TSGP	Transit Security Grant Program

U

UASI	Urban Areas Security Initiative
UAWG	Urban Area Working Group
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USDA	U.S. Department of Agriculture
UTL	Universal Task List

V

VRPP	Vulnerability Reduction Purchasing Plan

W

WMD	Weapons of Mass Destruction

X

XML	Extensible Markup Language
XSTF	XML Structure Task Force