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

FY 2006 Infrastructure Protection Program: *Transit Security*

Program Guidelines and Application Kit

Foreword

I am pleased to provide these FY 2006 program guidelines and application materials for the U.S. Department of Homeland Security (DHS) Infrastructure Protection Program.

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, respond to, and recover from threats to America's safety and security. The Directorate serves a strategic integration function of people, funding and programs.

The new Preparedness Directorate includes the essential work of the Department's Office of Grants and Training. 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 related infrastructure protection grants. The FY 2006 Transit Security Grant Program makes up $136 million of the total infrastructure protection grant funds available. These grants are a vital tool in making our nation safer in the war against 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 transit security:

- The Transportation Security Administration has the lead, except for Ferry systems where the Coast Guard will have the lead, for assuring that the grants accomplish key objectives such as aligning our grant making to the highest risk transportation facilities using refined risk- and need-based methods developed for grants. This process will hasten the development of an integrated risk-based decision making process for each regional area and agency, and will support implementation of the National Infrastructure Protection Plan (NIPP) and achievement of the National Preparedness Goal.

- The Department of Homeland Security's Office of Grants and Training provides design, facilitation, coordination and financial management administration for these programs. 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.

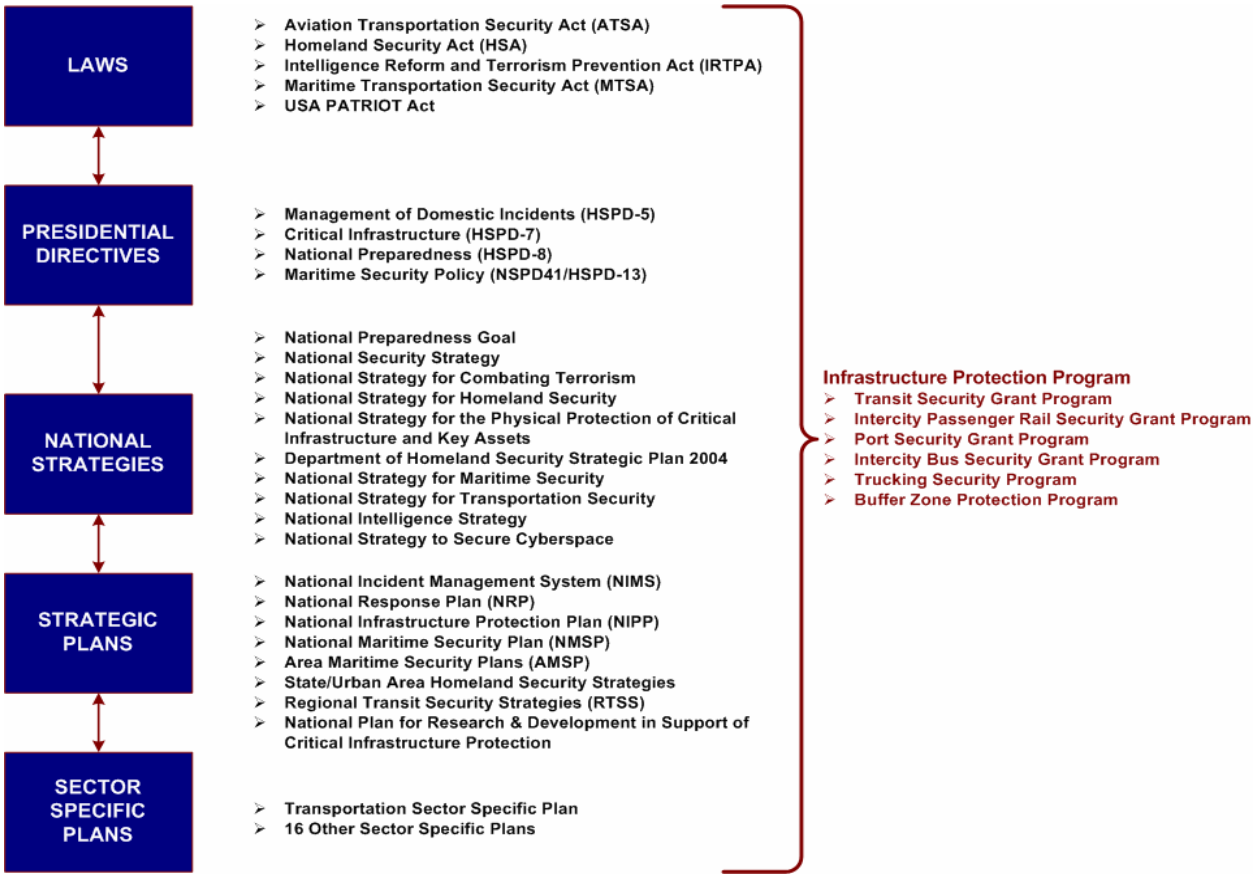
Michael Chertoff
Secretary
Department of Homeland Security

Contents

I. Introduction

The FY 2006 Transit Security Grant Program (TSGP) 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) outlined in Figure 1. Of particular significance are the National Preparedness Goal (the Goal) and its associated work products, the National Infrastructure Protection Plan (NIPP) and the National Strategy for Transportation Security (NSTS).

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



On March 31, 2005, DHS issued the 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 Transit Security Grant.

II. The FY 2006 Transit Security Grant Program

The mission of the FY 2006 Transit Security Grant Program is to create a sustainable, risk-based effort for the protection of critical transit infrastructure from terrorism, especially explosives and non-conventional threats that would cause major disruption to commerce and significant loss of life.

A. Program Overview

As a component of the Infrastructure Protection Program (IPP), the FY 2006 TSGP assists the Nation's transit systems in obtaining the resources required to support the Goal and the associated National Priorities. Through a risk-based approach focused on regional planning, infrastructure protection, improvised explosive devices (IEDs) and other non-conventional methods of attack, as well as training, exercises and citizen preparedness, the FY 2006 TSGP directly addresses six of the seven National Priorities:

1) Expanded regional collaboration;
2) Implementing National Incident Management System and the National Response Plan;
3) Implementing the NIPP;
4) Strengthening information sharing and collaboration capabilities;
5) Enhancing interoperable communications capabilities; and,
6) Strengthening CBRNE detection and response capabilities.

In addition, the FY 2006 TSGP also supports strengthening emergency operations planning and citizen protection capabilities, and assists in addressing security priorities specific to the transit sector.

B. Security Priorities Specific to the Intracity Rail Sector

Equipment acquisitions, drills and exercises, employee training programs, and public awareness programs that focus on mitigating the risk priorities represent appropriate use of rail TSGP funding. The following risk-based priorities should be addressed (as applicable):

(1) Protection of underwater and other deep bore tunnels and associated track mileage from attacks employing IEDs;

(2) Development and enhancement of capabilities to prevent, detect, and respond to terrorist attacks employing improvised explosive devices. IEDs pose a threat of great concern to transit systems and infrastructure across the Nation. They have historically been the terrorist weapon of choice because they combine a high degree of effectiveness with minimal cost. Capabilities to protect other assets besides tunnels should focus on passenger trains, stations with high passenger

throughput thru major urban areas, large rail yards, operations control centers, and high profile, high volume transit and rail bridges and tunnels; and

(3) Mitigation of other high consequence risks identified through individual transit system risk assessments.

The Federal Transit Administration (FTA) has established 20 specific action items for transit system security readiness. Implementation of these action items enhances security posture generally and supports achievement of the National Preparedness Goal and national and regional strategies to mitigate risk. Eligible applicants are encouraged to review these action items and adopt those currently missing from their security program.

The current version of the 20 action items may be accessed at the "Safety and Security" section of the FTA website. The action items and supporting references provide an excellent resource to facilitate development of passenger rail system security plans and programs. Passenger rail owners and operators should periodically review the FTA website for updates to program action items and supplements to the supporting reference materials.

Of note, the action items are being revised in a joint effort by FTA, TSA, and DHS to emphasize current security priorities. The revision will provide guidance to TSA's Surface Transportation Security Inspectors for monitoring the voluntary implementation by industry.

C. Security Priorities Specific to the Intracity Bus Sector

Equipment acquisitions, drills and exercises, employee training programs, and public awareness programs that focus on mitigating the risk priorities represent appropriate use of Intracity bus TSGP funding. The following risk-based priorities should be addressed (as applicable):

(1) Development and enhancement of capabilities to improve inventory control, such as ignition key-recognition systems and remote tracking/shut-down capabilities. The use of intracity buses as a weapon poses a threat of great concern to intracity bus systems and critical infrastructure;

(2) Increased perimeter security at intracity bus depots and yards. Related to the first priority, access control at areas of storage is an effective way to deter the use of intracity buses as a vehicle borne IED;

(3) Development and enhancement of training and awareness among intracity bus operators and employees. Training and awareness should cover the detection and deterrence of efforts by terrorists to use intracity buses as a means to attack critical infrastructure and key resources, in addition to current efforts to deter attacks on the bus as the end target;

(4) Development of emergency response and preparedness capabilities in the event an intracity bus used as a weapon to inflict damage on critical infrastructure;

(5) Implementation of technology-driven surveillance (e.g., CCTV). Technology-driven surveillance, either at intracity bus facilities or within the buses, can increase the effectiveness of other detection and deterrence measures; and

(6) Suspicious activity detection and behavior pattern recognition.

The FTA security program action items in Appendix E apply to Intracity buses as well as rail.

Appendix E provides a copy of the FTA Top 20 Security Program Action Items, as well as examples of practices that address these priorities.

D. Application Review Process and Project Selection Criteria for Intracity Rail and Bus Grants

The FY 2006 TSGP will use risk-based prioritization consistent with DHS policy. The Intracity Rail and Bus Grants will be awarded using a two tiered approach. Grants will be awarded in the first tier to regions, and the regions will have 90 days afterward to submit detailed project plans to TSA for approval. Systems in the first tier may submit project plans as either regions or individual agencies. First tier regions are identified in Table 2 on page 11. Project plans for Tier 1 systems will be evaluated on the following factors:

- Ability to reduce risk of catastrophic events;,
- Overall effect on regional transit security;
- Cost effectiveness to include leveraging additional resources; and
- Ability to complete the proposed project within the proposed timeframes.

Grants for Tier 2 systems will be competitively awarded based on the following factors:

- Ability to reduce risk;
- Cost effectiveness to include leveraging additional resources; and
- Ability to complete the proposed project within the timeframes.

The following method of selection will be used to evaluate Tier 2 system projects:

1. Rail and Bus agencies will submit concept papers for consideration. These concept papers will be submitted through grants.gov.

2. Concept papers will be reviewed and scored by a Federal Interagency Working Group consisting of TSA, FTA, and the DHS Office of Grants and Training (G&T);

3. Projects that are accepted will be required to complete full project applications;

4. The Preparedness Directorate in conjunction with TSA will verify compliance with each of the administrative and eligibility criteria identified in the application kit;

5. TSA will review the Federal Interagency Working Group recommendations and make final selections for funding to G&T and the Secretary. DHS will brief all appropriate agencies on the final selections to ensure consensus and address any remaining issues

In considering project plans for Tier I submissions, and concept papers for Tier II submissions, preference in awarding grants will be given to regions and agencies that propose providing matching funds or operations assets. DHS plans to implement a matching grant program, similar to the port security program, for all FY 2007 transit grants.

Common criteria for all concept papers

In order to receive consideration for an invitation to apply for a Tier II grant the respondent must be able to convey an understanding of the security priorities established under the TSGP guidance. Each concept paper must explain how the proposed project would fit into the overall Infrastructure Protection Program, with particular attention to the ability of the grant to fund a complete project, the extent to which it maximizes the projects risk reduction and cost effectiveness. An agency's response should also illustrate the broader context of the project, such as its ability to leverage operational resources and local law enforcement. Such an explanation could include information on the governance structure overseeing the effort, a communications system plan, a deployment plan, an operations plan or training and exercises.

At a minimum, the concept paper must:

- Define the vision, goals and objectives for the risk reduction the respondent is ultimately trying to achieve and how the proposed project will fit into an overall effort to meet critical infrastructure security priorities, including integration into existing security protocols;
- Describe the specific needs and/or resource limitations that need to be addressed;
- Identify any potential partners and their roles and staffing requirements, and provide information on any existing agreements such as Memorandums of Understanding (MOU);
- Propose a detailed budget and timeline; and
- Adhere to a maximum limit of five (5) pages.

E. Security Priorities Specific to the Ferry Sector

Equipment acquisitions, drills and exercises, employee training programs, and public awareness programs that focus on mitigating the risk priorities represent appropriate use of Ferry Security TSGP funding. The following risk-based priorities should be addressed (as applicable):

(1) Development and enhancement of capabilities to prevent, detect, and respond to terrorist attacks employing improvised explosive devices and vehicle borne improvised explosive devices. IEDs and VBIEDs pose a threat of great concern to ferry systems and infrastructure across the Nation;

(2) Mitigation of other high consequence risks identified through individual ferry system risk assessments;

(3) Use of K9 teams at the embarkation and exit points of a system as well as during passage;

(4) Innovative utilization of mobile technology for prevention and detection of explosives or other threats and hazards. This may include implementation of technology-driven surveillance (e.g., CCTV);

(5) Development and enhancement of physical and perimeter security capabilities to deny access around maintenance facilities, dry docks, and piers;

(6) Development and enhancement of training and awareness among ferry operators and employees. Training and awareness should cover the detection and deterrence of efforts by terrorists to use ferries as a means to attack critical infrastructure and key resources;

(7) Development of emergency response and preparedness capabilities or drills in the event of a ferry being used as a weapon to inflict damage on critical infrastructure (e.g., proximate LNG terminals and vital cargo shipping lanes); and

(8) Citizen awareness training.

F. Application Review Process and Project Selection Criteria for Ferry Grants

The FY 2006 TSGP will use risk-based prioritization consistent with DHS policy. The following method of selection will be followed under this program:

1. The Preparedness Directorate in conjunction with TSA will verify compliance with each of the administrative and eligibility criteria identified in the application kit;

2. Eligible applications will be reviewed and scored by a Federal Interagency Working Group consisting of TSA, FTA, USCG, and the DHS Office of Grants and Training (G&T);

3. TSA will review the Federal Interagency Working Group recommendations and make recommendations for funding to G&T and the Secretary. DHS will brief all appropriate agencies on the final selections to ensure consensus and address any remaining issues.

III. Funding Availability & Eligible Applicants

A. Funding Availability

The Preparedness Directorate, in conjunction with TSA, will award the available funds to projects offering the greatest risk reduction potential in the Nation's highest risk areas, thereby ensuring the funds are allocated to protect assets of the highest strategic importance nationally. Furthermore, the systems are listed alphabetically by state – no additional significance should be attributed to this ordering.

The Governor of each state and territory has designated a state administrative agency (SAA) to administer DHS funds. Accordingly, the relevant SAA will be the recipient of the funds awarded and responsible for the disbursement of the funds to the grantees.

Table 1 below summarizes the funding available through the FY 2006 TSGP by mode.

Table 1. FY 2006 TSGP Funding by Mode (Millions)

Transportation Mode	FY 2006 Funding
Tier I: Rail Transit	$103
Tier II: Rail Transit	$7
Tier I: Intracity Bus	$15
Tier II: Intracity Bus	$6
Ferry	$5

B. Regional Allocations

As part of the FY 2006 TSGP, DHS will use a risk-based approach to allocate TSGP funding on a regional basis. This approach will apply TSGP resources to generate the highest return on investment and, as a result, strengthen the security of the Nation's transit systems in the most effective and efficient manner.

The rail transit systems were divided into two tiers based on risk. Particular emphasis was placed on the passenger volume of the system and the underwater and underground infrastructure of the rail transit systems. Tier I systems are eligible for a regional allocation. Systems may apply as individual agencies or submit regional projects which mitigate the vulnerability of high risk, high consequence assets. Eligible

systems have to submit project plans to expend the allocated funds within 90 days. Eligible project plans include pilot programs (additional information on pilot programs is available at page 26), and other projects that address the priorities listed. Grants for systems in Tier II will be competitively awarded based on these factors: ability to reduce risk, cost effectiveness, and the ability to complete the proposed project with the funds awarded (as described in more detail in Part II).

The bus transit systems were divided into two tiers based on risk as well. Particular emphasis was placed on ridership, passenger miles, and the number of buses in the system. Tier I systems were awarded allocations that are shown in Table 3. Grants for bus systems in Tier II will be competitively awarded based on the same factors (described more fully in Part II) of ability to reduce risk, cost effectiveness, and likelihood of project completion using the funds awarded.

C. Eligible Applicants

Tables 2 through 4 identify systems for TSGP funds. Please note that presence on this list does not guarantee the receipt of grant funding.

1. **Rail Transit.** Table 2 identifies the eligible rail transit systems for Tier 1 and 2. Eligible systems were determined using a risk-based formula. Tier 1 systems appear in bold.

Table 2. Eligible Rail Transit Systems

State	Urban Area	FY 2006 Regional Allocation	Eligible System	Eligible Mode
CA	**Bay Area**	**$8.4M**	Peninsula Corridor Joint Powers Board	Commuter Rail
			San Francisco Bay Area Rapid Transit District	Heavy Rail
			Altamont Commuter Express	Commuter Rail
			Santa Clara Valley Transportation Authority	Light Rail
			San Francisco Municipal Railway	Commuter Rail, Light Rail
	Greater Los Angeles Area (Los Angeles/Long Beach and Anaheim/Santa Ana UASI Areas)	**$4.0M**	Southern California Regional Rail Authority (Metrolink)	Commuter Rail
			Los Angeles County Metro Transportation Authority	Heavy Rail, Light Rail
	Sacramento	Tier 2	Sacramento Regional Transit District	Light Rail
	San Diego	Tier 2	North San Diego County Transit District	Commuter Rail
			San Diego Trolley, Inc.	Light Rail
CO	Denver	Tier 2	Denver Regional Transportation District	Light Rail
DC/MD/VA[1]	**Greater National Capital Region (NCR and Baltimore UASI Areas)**	**$13.0M**	Washington Metropolitan Area Transit Authority	Heavy Rail
			Virginia Railway Express	Commuter Rail
			Maryland Transit Administration	Commuter Rail, Heavy Rail, Light Rail

[1] The DC SAA will administer these funds

State	Urban Area	FY 2006 Regional Allocation	Eligible System	Eligible Mode
FL	Jacksonville	Tier 2	Jacksonville Transportation Authority	Other Rail (AG)
	Miami/Fort Lauderdale	Tier 2	Tri-County Commuter Rail	Commuter Rail
			Miami-Dade Transit	Heavy Rail, Other Rail (AG)
GA	**Atlanta**	**$2.0M**	Metropolitan Atlanta Rapid Transit Authority	Heavy Rail
IL/IN[1]	**Chicago**	**$11.0M**	Northeast Illinois Regional Commuter Railroad Corporation	Commuter Rail
			Chicago Transit Authority	Heavy Rail
			Northern Indiana Commuter Transportation District	Commuter Rail
LA	New Orleans	Tier 2	New Orleans Regional Transit Authority	Light Rail
MA	**Boston**	**$9.6M**	Massachusetts Bay Transportation Authority	Commuter Rail, Heavy Rail, Light Rail
MI	Detroit	Tier 2	City of Detroit Department of Transportation	Other Rail (AG)
MN	Twin Cities Area	Tier 2	Metro Transit	Light Rail
MO	Saint Louis	Tier 2	Bi-State Development Agency	Light Rail
NY	Buffalo	Tier 2	Niagara Frontier Transp. Authority	Light Rail
NY/NJ/CT[3]	**New York City/Jersey City/Newark**	**$47.0M**	Metropolitan Transportation Authority	Heavy Rail, Commuter Rail
			Port Authority of New York and New Jersey	Heavy Rail
			New Jersey Transit Corporation	Light Rail, Commuter Rail
			Connecticut Department of Transportation	Commuter Rail
OH	Cleveland	Tier 2	The Greater Cleveland Regional Transit Authority	Heavy Rail, Light Rail
OR	Portland	Tier 2	Tri-County Metropolitan Transportation District of Oregon	Light Rail
PA	Pittsburgh	Tier 2	Cambria County Transit Authority	Other Rail (IP)
			Port Authority of Allegheny County	Light Rail, Other Rail (IP)
PA/NJ	**Philadelphia**	**$8.0M**	Pennsylvania Department of Transportation	Commuter Rail
			Southeastern Pennsylvania Transportation Authority	Commuter Rail, Heavy Rail, Light Rail
			Port Authority Transit Corporation	Heavy Rail
			New Jersey Transit Corporation	Commuter Rail
TN	Memphis	Tier 2	Memphis Area Transit Authority	Light Rail
TX	Dallas/Fort Worth/Arlington	Tier 2	Dallas Area Rapid Transit	Light Rail
			Trinity Railway Express	Commuter Rail
	Houston	Tier 2	Metropolitan Transit Authority Of Harris County	Light Rail
WA	Seattle	Tier 2	Central Puget Sound Regional Transit Authority	Commuter Rail, Light Rail

Note: "Other Rail" Includes:

- ***Automated Guideway (AG)***
- ***Cable Car (CC)***
- ***Inclined Plane (IP)***

[1] The IL SAA will administer these funds
[3] The NY SAA will administer these funds

2. **Intracity Bus Transit.** Table 3 identifies the eligible bus transit systems. Tier I systems and their allocations are bolded.

Table 3. Eligible Intracity Bus Systems

State	Urban Area	FY 2006 Regional Allocation	Eligible System
AZ	Phoenix		Valley Metro Regional Public Transportation Authority
			City of Phoenix Public Transit Department
CA	**Bay Area**	**$2.1M**	Alameda-Contra Costa Transit District
			Golden Gate Bridge, Highway and Transportation District
			San Francisco Bay Municipal Transportation Authority
			Santa Clara Valley Transportation Authority
			Central Contra Costa Transit Authority
			San Mateo County Transit District
			Caltrans (Transbay Bus Terminal)
	Greater Los Angeles Area (Los Angeles/Long Beach and Anaheim/Santa Ana UASI Areas)	**$2.2M**	Los Angeles County Metro Transportation Authority
			Orange County Transportation Authority
			City of Los Angeles Department of Transportation
			Foothill Transit
			Santa Monica's Big Blue Bus
			Long Beach Transit
	San Diego	Tier 2	San Diego Metropolitan Transit System
			North San Diego County Transit District
CO	Denver	Tier 2	Denver Regional Transportation District
DC/MD/VA	**Greater National Capital Region (NCR and Baltimore UASI Areas)**	**$1.3M**	Washington Metropolitan Area Transit Authority
			Maryland Transit Administration
			Ride-On Montgomery County Transit
			Prince George's County Transit
			City of Alexandria - Alexandria Transit Company
			Fairfax Connector Bus System
			Potomac and Rappahannock Transportation Commission
FL	Miami/Fort Lauderdale	Tier 2	Miami-Dade Transit
			Broward County Mass Transit Division

State	Urban Area	FY 2006 Regional Allocation	Eligible System
GA	Atlanta	Tier 2	Metropolitan Atlanta Rapid Transit Authority
			Georgia Regional Transportation Authority
HI	Honolulu	Tier 2	City and County of Honolulu Department of Transportation Services
IL/IN	**Chicago**	**$1.5M**	Chicago Transit Authority
			Pace - Suburban Bus Division
LA	New Orleans	Tier 2	New Orleans Regional Transit Authority
			Jefferson Parish Department of Transit Administration
MA	**Boston**	**$1.0M**	Massachusetts Bay Transportation Authority
MI	Detroit	Tier 2	City of Detroit Department of Transportation
			Suburban Mobility Authority for Regional Transportation
MN	Twin Cities Area	Tier 2	Metro Transit
MO	St. Louis	Tier 2	Bi-State Development Agency
			Madison County Transit District
NV	Las Vegas	Tier 2	Regional Transportation Commission of Southern Nevada
NY/NJ/CT	**New York City/Jersey City/Newark**	**$5.5M**	Metropolitan Transportation Authority
			New Jersey Transit Corporation
			Westchester County Department of Transportation
			Port Authority of New York and New Jersey (PANYNJ Manhattan Bus Terminals)
OH	Cincinnati	Tier 2	Southwest Ohio Regional Transit Authority
			Transit Authority of Northern Kentucky
	Cleveland	Tier 2	The Greater Cleveland Regional Transit Authority
OR	Portland	Tier 2	Tri-County Metropolitan Transportation District of Oregon
			Clark County Public Transportation Benefit Area Authority
PA	Pittsburgh	Tier 2	Port Authority of Allegheny County
PA/NJ	**Philadelphia**	**$1.4M**	Southeastern Pennsylvania Transportation Authority
			New Jersey Transit Corporation
TX	Dallas/Forth Worth/Arlington	Tier 2	Dallas Area Rapid Transit
			Ft. Worth Transportation Authority
	Houston	Tier 2	Metropolitan Transit Auth. Of Harris County
			Island Transit
	San Antonio	Tier 2	VIA Metropolitan Transit
WA	Seattle	Tier 2	King County Department of Transportation - Metro Transit Division
			Pierce County Transportation Benefit Area Authority
			Snohomish County Transportation Benefit Area Corporation
WI	Milwaukee	Tier 2	Milwaukee County Transit System

New Urban Areas Eligible in FY 2006 for TSGP

New Transit Systems Eligible in FY 2006 for TSGP

3. **Ferry Transit.** Table 4 identifies the eligible ferry transit systems. Eligible systems and their funding were determined using a risk-based formula.

Table 4. Eligible Ferry Systems

State	Urban Area	FY 2006 Regional Allocation	Eligible System
CA	Bay Area	$0.7M	Golden Gate Bridge, Highway and Transportation District
			City of Alameda Ferry Services (Blue and Gold Lines Fleet)
			City of Vallejo Transportation Program
LA	New Orleans	$0.3M	Crescent City Connection Division - Louisiana Department of Transportation
MA	Boston	$0.4M	Massachusetts Bay Transportation Authority
NY/NJ	New York City	$1.3M	New York City Department of Transportation
			Port Authority of Trans Hudson Corporation
TX	Houston	$0.3M	Texas DOT (Bolivar Roads Ferry)
WA	Seattle	$2.0M	Washington State Ferries

New Transit Systems Eligible in FY 2006 for TSGP

IV. Program and Application Requirements

A. General Program Requirements

Grant Funds. The SAA must obligate at least **97 percent** of the funds awarded to designated transit systems within **60 days of the receipt of funds**[2]. A maximum of **3 percent** may be retained by the SAA, and any funds retained are to be used solely for management and administrative (M&A) purposes. In addition, transit agencies receiving pass-through funds may also use up to **2.5 percent of their sub-award** for M&A purposes.

B. Specific Program Requirements

The SAA, will be responsible for administration of the FY 2006 TSGP. In administering the program, the SAA must work with the RTSWG and eligible transit systems to comply with the following requirements:

1. **Update the Regional Transit Security Strategy.** Transit systems eligible for funding may participate in an RTSWG for the purpose of aligning their RTSS with the Goal and the National Priorities. In addition, RTSWGs should also review the RTSS to ensure it adequately addresses the following priorities specific to transit security: 1) the protection of any underwater tunnels and associated track mileage from IED attacks; 2) prevention and detection capabilities for IEDs and other non-conventional weapons generally; 3) other high consequence risks identified through system-wide risk assessments; 4) anti-terrorism training for transit employees; 5) emergency drills; and, 6) citizen awareness activities. RTSWGs must also ensure that each RTSS continues to align with the goals and objectives contained within the relevant state and urban area strategy(ies).

C. Application Requirements

The following steps must be completed using the on-line Grants.gov system to ensure a successful application submission:

1. **Application Process**

   DHS 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, DHS is requiring that all discretionary, competitive grant programs be***

administered through Grants.gov. Eligible applicants must apply for FY 2006 TSGP funding through Grants.gov at http://www.grants.gov. Complete Applications must be received by G&T no later than August 4, 2006 at 11:59pm Eastern Standard Time.

2. On-Line Application

The on-line application must be completed and submitted using Grants.gov. The on-line application replaces the following previously required paper forms:

Standard Form 424, Application for Federal Assistance;
- Standard Form LLL, Disclosure of Lobbying Activities;
- OJP Form 4000/3, Assurances;
- OJP form 4061/6, Certifications;
- Non-Supplanting Certification.

The program title listed in the Catalog of Federal Domestic Assistance (CFDA) is "*Rail and Transit Security Grant Program."* The CFDA number is **97.075**. When completing the on-line application, applicants should identify their submissions as new, non-construction applications. It is important to note that this is a procedural requirement within Grants.gov and does not prohibit the applicant from submitting construction projects. The project period will be for a period not to exceed **30 months**.

3. National Environmental Policy Act (NEPA)

NEPA requires G&T to analyze the possible environmental impacts of each construction project. The purpose of a NEPA review is to weigh the impact of major Federal actions or actions undertaken using Federal funds on adjacent communities, water supplies, historical buildings, endangered species, or culturally sensitive areas prior to construction. Grantees wishing to use G&T funding for construction projects must complete and submit a NEPA Compliance Checklist to G&T for review. Additionally, grantees may be required to provide additional detailed information on the activities to be conducted, locations, sites, possible construction activities, possible alternatives, and any environmental concerns that may exist. Results of the NEPA Compliance Review could result in a project not being approved for G&T funding, the need to perform an Environmental Assessment (EA) or draft an Environmental Impact Statement (EIS). This information may be provided using one of the attachment fields within Grants.gov.

Appendix F provides a copy of the NEPA checklist.

4. Use of a Universal Identifier by Grant Applicants.

The applicant must provide a Dun and Bradstreet (D&B) Data Universal Numbering System (DUNS) number with the application. An application

will not be considered complete until a valid DUNS number is provided by the applicant. ***This number is a required field within Grants.gov.*** Organizations should verify that they have a DUNS number or take the steps necessary to obtain one as soon as possible.

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

5. Freedom of Information Act (FOIA)

G&T recognizes that much of the information submitted in the course of applying for funding under this program, or provided in the course of its grant management activities, may be considered law enforcement sensitive or otherwise important to national security interests. This may include threat, risk, and needs assessment information, and discussions of demographics, transportation, public works, and industrial and public health infrastructures. While this information under Federal control is subject to requests made pursuant to the 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 Protected Critical Infrastructure Information (6 CFR Part 29) and Sensitive Security Information (49 CFR Part 1520), as these designations may provide additional protection to certain classes of homeland security information.

6. 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 the following: 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.

7. 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. USC 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 USC 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 USC 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 USC 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 its compliance with these laws and their implementing regulations.

8. Financial Requirements

Non-Supplanting Certification: This certification affirms that these grant funds will be used to supplement existing funds, and will not replace (supplant) funds that have been appropriated for the same purpose. Potential supplanting will be addressed in the application review, as well as in the pre-award review, post-award monitoring and any potential audits. Applicants or grantees may be required to supply documentation certifying that a reduction in non-Federal resources occurred for reasons other than the receipt or expected receipt of Federal funds.

- **Accounting System and Financial Capability Questionnaire:** All non-governmental (non-profit and commercial) organizations that apply for funding with G&T that have not previously (or within the last three years) received funding from G&T must complete the Accounting System and Financial Capability Questionnaire. ***This information may be provided using one of the attachment fields within the on-line Grants.gov application.***

  The required form can be found at http://www.ojp.usdoj.gov/oc.

- **Assurances:** Assurances forms (SF-424B and SF-424D) can be accessed at http://apply.grants.gov/agency/FormLinks?family=7. It is the responsibility of the recipient of the Federal funds to fully understand and comply with these requirements. Failure to comply may result in the withholding of funds, termination of the award, or other sanctions. The applicant will be agreeing to these assurances upon the submission of the application.

- **Certifications Regarding Lobbying; Debarment, Suspension, and Other Responsibility Matters; and Drug-Free Workplace Requirement:** This certification, which is a required component of the on-line application, commits the applicant to compliance with the certification requirements under 28 CFR part 67, *Government-wide Debarment and Suspension (Non-procurement);* 28 CFR part 69, *New Restrictions on Lobbying;* and 28 CFR part 83 *Government-wide Requirements for Drug-Free Workplace (Grants)*. All of these can be referenced at: http://www.access.gpo.gov/nara/cfr/waisidx_04/28cfrv2_04.html.

  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.

9. Services to Limited English Proficient (LEP) Persons

Recipients of G&T financial assistance are required to comply with several Federal civil rights laws, including Title VI of the Civil Rights Act of 1964, as amended. These laws prohibit discrimination on the basis of race, color, religion, national origin, and sex in the delivery of services. National origin discrimination includes discrimination on the basis of limited English proficiency. To ensure compliance with Title VI, recipients are required to take reasonable steps to ensure that LEP persons have meaningful access to their programs. Meaningful access may entail providing language assistance services, including oral and written translation, where necessary. 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, please see http://www.lep.gov.

10. 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, non-governmental organizations, and the general public in the implementation of emergency preparedness plans as they relate to individuals with disabilities. A January 2005 letter to state governors from then-Homeland Security Secretary Tom Ridge asked states to consider several steps in protecting individuals with disabilities:

- Ensure that 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 http://www.dhs.gov/disabilitypreparedness. This resource center provides information to assist emergency managers in planning and response efforts related to people with disabilities. In addition, 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.

11. Public Awareness and Citizen Participation

Citizens are a critical component of homeland security, and to have a fully prepared community, citizens must be fully aware, trained, and practiced on how to detect, deter, prepare for, and respond to emergency situations. Recent surveys indicate that citizens are concerned about the threats facing the Nation and are willing to participate to make their communities safer, yet most Americans have low awareness of Federal, state, and local emergency preparedness plans, are not involved in local emergency drills, and are not adequately prepared at home.

Informed and engaged citizens are an essential component of homeland security and the mission of Citizen Corps is to have everyone in America participate in making their community safer, stronger, and better prepared. To achieve this, state, local and tribal Citizen Corps Councils have formed nationwide to help educate and train the public, and to develop citizen/volunteer resources to support local emergency responders, community safety, and disaster relief.

DHS and DOT are currently working to align the Citizen Corps and Transit Watch programs. In support of this initiative, and consistent with the priority that must be given to public awareness, FY 2006 TSGP award recipients should work with the applicable state and local Citizen Corps Councils to more fully engage citizens through the following activities:

- **Expand plans and task force memberships to address citizen participation.** Develop or revise plans to integrate citizen/volunteer resources and participation, and include advocates for increased citizen participation in task forces and advisory councils;

- **Awareness and outreach to inform and engage the public.** Educate the public on personal preparedness measures, terrorism awareness, alert and warning systems, and state and local emergency plans via a range of community venues and communication channels;

- **Include citizens in training and exercises.** Provide emergency preparedness and response training for citizens, improve training for emergency responders to better address special needs populations, and involve citizens in all aspects of emergency preparedness exercises, including planning, implementation, and after action review;

- **Develop or expand programs that integrate citizen/volunteer support for the emergency responder disciplines.** Develop or expand Citizen Corps Programs into the rail environment, including citizen participation in prevention and response activities;

In addition, FY 2006 TSGP award recipients should also take advantage of the public awareness materials developed through Transit Watch. To facilitate this, ***reproduction of official Transit Watch materials is an allowable expense as part of this program.***

12. Transit Safety and Security Roundtables and Connecting Communities

As part of its post-9/11 security initiative, FTA developed the Transit Safety and Security Roundtables and Connecting Communities programs. The Transit Safety and Security Roundtables offer a mechanism for transit safety and security leaders to share information on technology, best practices and available resources, as well as develop relationships between Federal and local officials working in the area of public transportation safety and security. The Connecting Communities forums offered to a community's transit managers and security

personnel, emergency management coordinators, fire response and police personnel, emergency medical services and hospital disaster relief coordinators, among others. Each Connecting Communities forum involves hands-on exercises, discussions, emergency scenarios, group break-out sessions, and presentations, and provides community officials with the opportunity to network and coordinate on emergency response, learn about the role of transit and alternative means of transportation during an emergency, and identify the elements, facilities, and personnel in their community needed for effective emergency response. FTA, TSA and G&T are currently working to develop a process for jointly sponsoring and continuing these important programs. ***In support of this, FY 2006 TSGP funding may be used to cover the costs of invitational travel to future Transit Safety and Security Roundtables, as well as for overtime and backfill costs associated with attending locally delivered Connecting Communities forums.***

13. Training

FTA, TSA and G&T have developed and currently offer a variety of training programs that address transit security and emergency preparedness. FY 2006 TSGP funding may be used to attend and/or support the local delivery of many of these courses. The system agrees to share with the Department any training developed with grant funds.

Appendix A provides a listing of allowable training costs.

V. Assistance Resources and Support

A. Drawdown and Expenditure of Funds.

G&T's Office of Grant Operations (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 subgrant recipients should refer to the OGO *Financial Management Guide* or contact OGO at 1-866-9ASKOGO or ask-ogo@dhs.gov. All payment related questions should be referred to OJP/OC's Customer Service at 1-800-458-0786 or askoc@ojp.usdoj.gov. All grant and sub-grant recipients should refer to the OGO *Financial Management Guide*.

Following acceptance of the grant award and release of any special conditions withholding funds, the Grantee can drawdown and expend grant funds through the Automated Standard Application for Payments (ASAP), Phone Activated Paperless System (PAPRS) or Letter of Credit Electronic Certification System (LOCES) payment systems.

In support of our continuing effort to meet the accelerated financial statement reporting requirements mandated by the U. S. Department of the Treasury and the Office of Management and Budget (OMB), payment processing will be interrupted during the last five working days each month. Grantees 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 June, the last day to request (draw down) payments will be June 23, 2006. Payments requested after June 23, 2006, will be processed when the regular schedule resumes on July 3, 2006. A similar schedule will follow at the end of each month thereafter.

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 draw down funds up to 120 days prior to expenditure/disbursement, which echoes the recommendation of the Funding Task Force. G&T strongly encourages recipients to draw down funds as close to expenditure as possible to avoid accruing interest. ***Funds received by grantees must be placed in an interest-bearing account and are subject to the rules outlined in the Uniform Rule 28 CFR Part 66, Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments***, at: http://www.access.gpo.gov/nara/cfr/waisidx_04/28cfrv2_04.html and the Uniform Rule 28 CFR Part 70, Uniform Administrative Requirements for Grants and

Agreements (Including 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 Office of Grant Operations (OGO) will provide fiscal support and 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. Homeland Security Preparedness Technical Assistance Program

The Homeland Security Preparedness Technical Assistance Program (HSPTAP) provides technical assistance on a first-come, first-served basis (and subject to the availability of funding) to eligible organizations for enhancing their capacity and preparedness to respond to weapons of mass destruction (WMD) terrorist incidents. In addition to the risk assessment assistance already being provided, G&T also offers a variety of other technical assistance programs.

Further information on the HSPTAP can be found on G&T's web site at http://www.ojp.usdoj.gov/odp/ta.htm under the Catalog link, or by contacting the CSID.

E. Homeland Defense Equipment Reuse Program

The mission of the Homeland Defense Equipment Reuse (HDER) Program is to provide excess radiological detection instrumentation and other equipment, as well as training and technical support, to emergency responder agencies nationwide to immediately enhance their homeland security capabilities. The used but operable instrumentation provided through HDER constitutes a rapid, short-term solution to the immediate needs of emergency responders for this equipment. With the recent adoption of new ANSI standards, it is envisioned that new standards-based equipment will ultimately be substituted for HDER equipment as the new equipment becomes more widely available and as budgets allow.

For additional information on the equipment, training and technical support available through HDER, please contact the CSID at 1-800-368-6498.

F. 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 times, on-line 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 which can be initiated by contacting the appropriate program representative. Additional information on the programs and contact information for program representatives is available in fact sheets posted on the G&T website.

For information on the Emergency Responder Equipment Purchase Program run through DLA's Defense Supply Center Philadelphia, see http://www.ojp.usdoj.gov/odp/docs/fs-padef.htm.

G. Lessons Learned Information Sharing (LLIS) System

LLIS is a national, online secure network located at http://www.LLIS.gov that houses a collection of peer-validated lessons learned, best practices, after action reports (AAR) from exercises and actual incidents, and other relevant homeland security documents. LLIS is designed to help emergency response providers and homeland security officials prevent, prepare for, respond to, and recover from acts of terrorism. LLIS will improve preparedness nationwide by allowing response professionals to tap into a wealth of validated front-line expertise on effective planning, training, equipping, and operational practices for homeland security. The system also houses a 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.

H. TSA Surface Transportation Security Inspection Program

As a condition of receiving grants, Grantees will be required to provide SSTS's access to their facilities, tracks and vehicles and rolling stock.TSA has deployed Surface Transportation Security Inspectors (STSIs) to work with passenger rail owners and operators to evaluate the security procedures in place and enhance security of the passenger rail system. The foundational legislation for this program is the Department of Homeland Security Appropriations Acts for FY 2005 and FY 2006, which appropriated funds for the hiring and deployment of "Federal rail compliance inspectors" (FY 2005) and "rail inspectors" (FY 2006).

Pursuant to the Aviation and Transportation Security Act (ATSA) (Public Law 107-71), TSA is "responsible for security in all modes of transportation" (49 U.S.C. §114(d)). In meeting this responsibility, the Administrator of TSA is expressly empowered to assess threats to transportation (49 U.S.C. §114(f)(2)); develop policies, strategies, and plans for dealing with threats to transportation security (49 U.S.C. §114(f)(3)); enforce security requirements (49 U.S.C. §114(f)(7)); generally inspect, maintain, and test security facilities, equipment, and systems (49 U.S.C. §114(f)(9)); and ensure the adequacy of security of transportation facilities (49 U.S.C. §114(f)(11)). The Surface Transportation Security Inspection Program represents one means by which TSA implements this authority through compliance inspections and programs to enhance domain awareness and security posture throughout the passenger rail and mass transit mode.

The program focuses on nationwide outreach and liaison activities with the passenger rail and rail transit industry and initiatives aimed at enhancing security in passenger rail and mass transit systems. Inspectors are actively engaged in performing Security Analysis and Action Programs, which constitute a systematic examination of a stakeholder's operations to assess compliance with security requirements, identify security gaps, develop best practices for sharing across the mode, and gathering baseline information on the system, its operations, and its security resources and initiatives. System Security Evaluations assess a system's security posture

comprehensively. Security Directive Reviews are more targeted, assessing the status of compliance with the applicable TSA security directive (SD). Inspectors will also conduct reviews of the FTA/TSA Top 20 Security Program Action Items for Transit Agencies.

RTSWGs and individual transit systems should direct questions concerning integration of STSI program services into their security assessments to the regional or local inspector's office in their area. Questions may also be directed to sd.masstransit@dhs.gov.

I. TSA Explosive Detection Canine Program

An additional resource for enhancing IED prevention and detection capabilities is the TSA Explosives Detection Canine Team Program. ***The applicant is encouraged to explore the resources available through this program as a means of further enhancing its IED preventing and detection capabilities.***

The TSA Explosive Detection Canine Program is a partnership with industry in which airports and mass transit systems voluntarily participate and are supported by Federal funds in the amount of $40,000 per year, per canine team. The TSA pays to purchase and train the dogs, trains the canine handlers, and partially reimburses each participating agency for costs associated with maintaining the teams. Associated costs include handlers' salaries (handlers are usually airport police or local law enforcement personnel), food and veterinarian costs. In turn, the accepting agency agrees to utilize TSA canine teams at least 80 percent of the time in the transportation environment and to maintain a minimum of three certified teams available for around-the-clock incident response.

Each canine team, composed of one dog and one handler, undergoes 10-weeks of intensive training at the Transportation Security Administration Explosives Detection Canine Handler Course at Lackland Air Force Base in San Antonio, Texas. Once the teams are certified by the TSA, they undergo several hours of proficiency training each week in their operational environment, which includes all the smells and distractions associated with a busy airport or mass transit system. The TSA also requires each team to go through an intensive three to four day annual re-certification to demonstrate they continue to meet TSA-certification standards. These standards are some of the most stringent in the Nation and include demonstrated performances in searching aircraft, luggage, terminals, cargo and vehicles.

Inquiries concerning the TSA National Explosives Detection Canine Program should be addressed to:

Director, National Explosives Detection Canine Program
Headquarters Transportation Security Administration
601 South 12th Street (TSA-7)
Arlington, VA 22202-4220

E-mail: k-9@dhs.gov

VI. Reporting, Monitoring and Closeout Requirements

A. Reporting Requirements

The following reports are required of all program participants:

1. **Financial Status Reports (FSRs) – Standard Form 269a**

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

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

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

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

   For FY 2006 awards, grant and subgrant recipients should refer to the OGO Financial 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.

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

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

Following award of grant, the State and subgrantees will be responsible for providing updated obligation and expenditure information on a regular basis. ***The applicable SAAs are responsible for completing and submitting the CAPR/BSIR reports.*** The BSIR submission will satisfy the narrative requirement in Box 12 of the biannual Categorical Assistance Progress Report (CAPR – OJP Form 4587/1). SAAs will still be required to submit the CAPR form with a line in box 12 which reads: See BSIR.

The BSIR and the CAPR are due within 30 days after the end of the reporting period (July 30 with a reporting period of January 1 through June 30, and on January 30 with a reporting period of July 1 though December 31). Grantees will provide initial overall obligation and expenditure information with the CAPR/BSIR submission due January 30, 2007. 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 and a copy of the CAPR (OJP Form 4587/1) in the initial award package. ***Future awards and fund draw downs may be withheld if these reports are delinquent.***

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

Required Submission: CAPR/BSIR (biannually).

Important Note: While budget detail worksheets do not need to be submitted with the application, SAAs and transit agencies must maintain complete and accurate accounting records, and use that information in the preparation of the BSIR. In addition, these records must be available to DHS upon request.

Appendix G provides additional guidance on completing the BSIR.

3. Exercise Evaluation and Improvement

Exercises implemented with grant funds should be threat- and performance-based and should evaluate performance of critical prevention and response tasks required to respond to the exercise scenario. Guidance on conducting exercise evaluations and implementing improvement is defined in the *Homeland Security Exercise and Evaluation Program (HSEEP) Volume II: Exercise Evaluation and Improvement* located at http://www.ojp.usdoj.gov/G&T/docs/HSEEPv2.pdf. Recipients must report on scheduled exercises and ensure that an After Action Report (AAR) and Improvement Plan (IP) are prepared for each exercise conducted with G&T support (grant funds or direct support) and submitted to G&T within 60 days following completion of the exercise.

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

Required Submissions: AARs and IPs (as applicable).

4. Financial and Compliance Audit Report

Recipients that expend $500,000 or more of Federal funds during their fiscal year are required to submit an organization-wide financial and compliance audit report. The audit must be performed in accordance with the U.S. General Accountability Office, *Government Auditing Standards*, located at http://www.gao.gov/govaud/ybk01.htm, and *OMB Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations*, located at http://www.whitehouse.gov/omb/circulars/a133/a133.html. Audit reports are currently due to the Federal Audit Clearinghouse no later than nine months after the end of the recipient's fiscal year. In addition, the Secretary of Homeland Security and the Comptroller General of the United States shall have access to any books, documents, and records of recipients of FY 2006 TSGP 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.

B. Monitoring

Grant recipients will be monitored periodically by G&T program staff, OGO staff, TSA staff, and DHS Infrastructure Protection and TSA Surface Transportation Security Inspectors both programmatically and financially, to ensure that the project goals, objectives, timelines, budgets and other related program criteria are being met. Monitoring will be accomplished through a combination of office-based and on-site monitoring visits conducted jointly by preparedness and TSA (STSI) staff. Monitoring will involve the review and analysis of the financial, programmatic, and administrative issues relative to each program, and will identify areas where technical assistance and other support may be needed.

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

G&T will also implement a Mass Transit Homeland Security Assistance Program (MT/HSAP). The purpose of the MT/HSAP is to ensure that RTSWGs are aware of the full range of resources and support available from the Federal government to assist regions in making progress toward the goals and objectives identified in their RTSSs. The MT/HSAP process will include the following elements:

1. **Program Observations and Recommendations Report.** In coordination with its Federal partners, ***G&T*** will conduct detailed reviews of each RTSS and will develop a set of recommendations for implementing these strategies and addressing identified challenges. The product of this analysis will be a draft MT/HSAP Program Observations and Recommendations Report. In the report, ***G&T*** will detail both internal and external programs and linkages designed to assist in fully implementing the RTSS and overcoming identified challenges.

2. **Site Visit.** As an element of its Grant Monitoring Program, ***G&T*** will conduct site visits with each RTSWG through the Surface Transportation Security Inspection (STSI) Program. The focus of this portion of ***G&T***'s monitoring activities will be on discussing the RTSS and presenting the draft Program Observations and Recommendations Report. ***G&T*** will invite other pertinent Federal agencies and programs to ensure that appropriate expertise is available and that a holistic discussion of the RTSS and options can occur. ***G&T*** will finalize the Program Observations and Recommendations Report following the site visit and prepare a Transit Agency Assistance Plan. ***G&T***, again through the STSI Program, will monitor implementation of the Transit Agency Assistance Plan and coordinate the identified Federal support. TSA will provide Subject Matter Expertise where appropriate.

C. Grant Closeout Process

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

Required Submissions: 1) Final SF-269a, due 90 days from end of grant period; and, 2) Final CAPR/BSIR, due 90 days from the end of the grant period.

APPENDIX A

AUTHORIZED PROGRAM EXPENDITURES GUIDANCE

Authorized Program Expenditures Guidance

This appendix serves as a guide for program expenditure activities. Applicants are encouraged to contact their G&T Program Manager regarding authorized and unauthorized expenditures.

A. Projects that Support the National Transit Security Priorities

Within project proposals, specific attention must be paid to the prevention, detection, and response to incidents involving improvised explosive devices (IEDs). IEDs pose a threat of great concern to transit systems across the Nation. IEDs have historically been the terrorist weapon of choice because they combine a high degree of effectiveness with minimal cost. Eligible transit systems must leverage FY 2006 TSGP funding to develop capabilities to prevent, detect and respond to IED terrorist attacks. In addition, specific attention must also be paid to prevention, detection and response capabilities related to chemical, biological, radiological and nuclear (CBRN) devices.

The following are examples of security enhancements designed to enhance IED and chemical, biological radiological and nuclear prevention and detection capabilities for rail and intracity bus transit:

1. Operator/Vehicle Protection

- Explosive Agent Detection Sensors;
- Chemical/Biological/Radiological Agent Detection Sensors;
- Canines (Start-up Costs and Training);
- GPS Tracking Systems;
- On Board Camera Systems;
- Fixed Personnel Protection (driver shields, etc.);
- Interlock Security Devices;
- Kill Switch Technology; and,
- Interoperable Communications Systems.

2. Facility Security

- Explosive Agent Detection Sensors;
- Chemical/Biological/Radiological Agent Detection Sensors;
- Canines (Start-up Costs and Training);
- Blast Curtains;
- Intrusion Detection;
- Video Surveillance Systems;
- Secure Entry ID Systems;
- Employee Identification;
- Improved Lighting;
- Fencing and Secured Gates; and,
- Interoperable Communications Systems.

3. Training and Exercises

- Behavioral Screening Training for Frontline Employees;
- Anti-Terrorism Training;
- Anti-Hijacking Training;
- Public and Employee Awareness Programs;
- NIMS Training; and,
- Multi-disciplinary, Multi-jurisdictional Terrorism Exercises.

The following are examples of security enhancements designed to enhance IED and chemical, biological radiological and nuclear prevention and detection capabilities for ferry transit:

1. Ferry Terminals

- Explosive Agent Detection Sensors;
- Chemical/Biological/Radiological Agent Detection Sensors;
- Canines (Start-up Costs and Training);
- Intrusion Detection;
- Video Surveillance Systems;
- Security Entry/ID Systems;
- Employee Identification;
- Improved Lighting;
- Secure Gates and Vehicle Barriers;
- Floating Protective Barriers;
- Underwater Intrusion Detection Systems; and,
- Communications Equipment (including interoperable communications).

2. **Ferries**

   - Explosive Agent Detection Sensors;
   - Chemical/Biological/Radiological Agent Detection Sensors;
   - Restricted Area Protection (cipher locks, hardened doors, CCTV for bridges and engineering spaces);
   - Interoperable Communications Systems;
   - Canines (start-up costs and training for U.S. vehicle/passenger ferries); and,
   - Floating Protective Barriers.

3. **Training and Exercises**

   - Behavioral Screening Training for Frontline Employees;
   - Anti-Terrorism Training;
   - Anti-Hijacking Training;
   - Public and Employee Awareness Programs;
   - NIMS Training; and,
   - Multi-disciplinary, Multi-jurisdictional Terrorism Exercises.

B. Allowable Cost Guidance

FY 2006 TSGP allowable costs are divided into the following categories:

- *Planning*
- *Organizational Activities*
- *Equipment Acquisitions*
- *Training*
- *Exercises*
- *Management and Administration*

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

1. **Planning Costs.** FY 2006 TSGP funds may be used for the following types of planning activities:

   - Public Education/Outreach (such as reproduction of Transit Watch materials);

   - Development and implementation of homeland security support programs and adoption of ongoing DHS national initiatives;

   - Development and enhancement of plans and protocols;

   - Development or conduct of assessments;

- Hiring of full or part-time staff or contractors/consultants to assist with planning activities (not for the purpose of hiring public safety personnel);
- Conferences to facilitate planning activities;
- Materials required to conduct planning activities;
- Travel/per diem related to planning activities (such as attendance at Transit Safety and Security Roundtables); and,
- Other project areas with prior approval from G&T.

2. **Organizational Activities.** Transit agencies may use up to **25 percent** of their allocation to support operational overtime costs with written approval from G&T. This includes costs incurred during ***Code Orange*** and ***Code Yellow*** alerts (**MARSEC Level 1** or higher for eligible ferry systems) that are associated with increased security measures, as well as operational overtime costs that are associated with increased security measures incurred during ***National Security Special Events (NSSE)***, as designated by the Secretary of Homeland Security. Transit agencies may use funds for operational overtime costs associated with increased security measures at critical infrastructure sites and in the following authorized expenditure categories:

   - Backfill and overtime expenses for staffing emergency operations centers;
   - Hiring of contracted security for critical infrastructure sites; and,
   - Public safety overtime.

Important Note: This does not include consumable costs such as fuel expenses. In addition, funding for ferry services may not be used to supplant ongoing, routine public safety activities of state and local law enforcement, and may not be used to hire staff for operational activities or backfill.

3. **Equipment Acquisition Costs.** FY 2006 TSGP funds may be used for the following categories of equipment. A comprehensive listing of allowable equipment categories and types is found on the web-based Authorized Equipment List (AEL) on the Responder Knowledge Base (RKB) at http://www.rkb.mipt.org.

   - Personal Protection Equipment (PPE);
   - Explosive Device Mitigation and Remediation Equipment;
   - CBRNE Operational Search and Rescue Equipment;
   - Information Technology;
   - Cyber Security Enhancement Equipment;
   - Interoperable Communications Equipment;

- Detection Equipment;
- Decontamination Equipment;
- Medical Supplies and Limited Pharmaceuticals;
- Power Equipment;
- CBRNE Reference Materials;
- CBRNE Incident Response Vehicles;
- Terrorism Incident Prevention Equipment;
- Physical Security Enhancement Equipment;
- CBRNE Response Watercraft;
- CBRNE Logistical Support Equipment;
- Intervention Equipment; and,
- Other Authorized Equipment.

To help prevent and detect an event similar to the sarin gas attack on the Tokyo subway system, DHS, Department of Energy (DOE), National Institute of Justice (NIJ) and FTA collaborated on PROTECT (Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism), a systems approach to interior infrastructure protection for chemical incidents. PROTECT has been successfully demonstrated in Washington, DC and Boston.

PROTECT includes facility hardening, detection, emergency management information systems, transport modeling, engineering countermeasures and emergency response. The PROTECT program is aimed at providing an early warning crisis management system in the event of a chemical agent attack in a subway system. Chemical agent detectors are located in stations and activation is electronically reported to the Operations Control Center (OCC). Detector false alarms are eliminated by the requirement for redundancy of alarm activations and/or visual verification that the alarms coincide with patron distress. Response takes place in terms of halting of trains, shutting off station and tunnel ventilation, activation of pedestrian displays, public address announcements, and/or evacuation of critical stations and notification of outside responders. The system is invisible to patrons and may also be used for other emergencies (due to advanced video coverage capability). Responders, such as emergency managers in the OCC and the Incident Commander, can access the PROTECT system through fireman jacks and web connections. These provide: (a) detector alarms at the time of activation; (b) video views of stations under attack; (c) hazard zones above and below ground; (d) response recommendations for police, fire and other responders optimized for the type and size of attack; (e) train locations on a 1-sec updated basis; and, (f) a record of actions already taken by other responders. This information ensures a timely well coordinated response to effectively mitigate a chemical incident.

Currently, the FTA is compiling technology transfer documentation for PROTECT. In addition, technologies related to PROTECT are an allowable expense through the FY 2006 TSGP. For additional information on PROTECT, contact:

Lance Brooks
Portfolio Manager
Science and Technology Directorate
Department of Homeland Security
Phone: (202) 254-5768
Email: lance.brooks@dhs.gov

4. **Training Costs.** FY 2006 TSGP funds may be used for the following training activities:

- **Training Workshops and Conferences** - Grant funds may be used to plan and conduct training workshops or conferences to include costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, travel and training plan development;

- **Full or Part-Time Staff or Contractors/Consultants** - Full or part-time staff may be hired to support training-related activities. The services of contractors/ consultants may also be procured by the state in the design, development, conduct, and evaluation of CBRNE training. The applicant's formal written procurement policy or the Federal Acquisition Regulations (FAR) must be followed;

- **Overtime and Backfill Costs –** Payment of overtime expenses will be for work performed by award (SAA) or sub-award employees in excess of the established work week (usually 40 hours). Further, overtime payments and backfill costs associated with sending personnel to training are allowable, provided that it is G&T approved training. These costs are allowed only to the extent the payment for such services is in accordance with the policies of the state or unit(s) of local government and has the approval of the state or the awarding agency, whichever is applicable. In no case is dual compensation allowable. That is, an employee of a unit of government may not receive compensation from their unit or agency of government AND from an award for a single period of time (e.g., 1:00 pm to 5:00 pm), even though such work may benefit both activities. Fringe benefits on overtime hours are limited to Federal Insurance Contributions Act (FICA), Workers' Compensation and Unemployment Compensation;

- **Travel** - Travel costs (i.e., airfare, mileage, per diem, hotel, etc.) are allowable as expenses by employees who are on travel status for official business related to the planning and conduct of the training project(s) or for attending G&T-approved courses. These costs must be in accordance with state law as highlighted in the OGO *Financial Management Guide*. For further information on Federal law pertaining to travel costs please

refer to the OGO *Financial Management Guide*, available at http://www.dhs.gov/dhspublic/display?theme=18&content=4206;

- **Supplies** - Supplies are items that are expended or consumed during the course of the planning and conduct of the training project(s) (e.g., copying paper, gloves, tape, and non-sterile masks);

- **Other Items** - These costs include the rental of space/locations for planning and conducting training, badges, etc.

5. **Exercise Costs.** FY 2006 TSGP funds may be used for the following exercise activities:

   - **Exercise Planning Workshop -** Grant funds may be used to plan and conduct an Exercise Planning Workshop to include costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, travel and exercise plan development;

   - **Full or Part-Time Staff or Contractors/Consultants -** Full or part-time staff may be hired to support exercise-related activities. Payment of salaries and fringe benefits must be in accordance with the policies of the state or unit(s) of local government and have the approval of the state or the awarding agency, whichever is applicable. The services of contractors/consultants may also be procured to support the design, development, conduct and evaluation of CBRNE exercises. The applicant's formal written procurement policy or the Federal Acquisition Regulations (FAR) must be followed;

   - **Overtime and Backfill Costs –** Overtime and backfill costs associated with the design, development and conduct of CBRNE exercises are allowable expenses. Payment of overtime expenses will be for work performed by award (SAA) or sub-award employees in excess of the established work week (usually 40 hours) related to the planning and conduct of the exercise project(s). Further, overtime payments and backfill costs associated with sending personnel to exercises are allowable, provided that the event being attended is a G&T sponsored exercise. These costs are allowed only to the extent the payment for such services is in accordance with the policies of the state or unit(s) of local government and has the approval of the state or the awarding agency, whichever is applicable. In no case is dual compensation allowable. That is, an employee of a unit of government may not receive compensation from their unit or agency of government AND from an award for a single period of time (e.g., 1:00 pm to 5:00 pm), even though such work may benefit both activities. Fringe benefits on overtime hours are limited to FICA, Workers' Compensation and Unemployment Compensation;

   - **Travel -** Travel costs (i.e., airfare, mileage, per diem, hotel, etc.) are allowable as expenses by employees who are on travel status for official

business related to the planning and conduct of the exercise project(s). These costs must be in accordance with state law as highlighted in the OGO *Financial Management Guide*. States must also follow state regulations regarding travel. If a state or territory does not have a travel policy they must follow Federal guidelines and rates, as explained in the OGO *Financial Management Guide*. For further information on Federal law pertaining to travel costs please refer to http://www.dhs.gov/dhspublic/display?theme=18&content=4206

- **Supplies -** Supplies are items that are expended or consumed during the course of the planning and conduct of the exercise project(s) (e.g., copying paper, gloves, tape, non-sterile masks, and disposable protective equipment);

- **Other Items -** These costs include the rental of space/locations for exercise planning and conduct, exercise signs, badges, etc.

6. **Management and Administration (M&A) Costs.** FY 2006 TSGP funds may be used for the following M&A costs:

   - Hiring of full-time or part-time staff or contractors/consultants:

     - To assist with the management of the FY 2006 TSGP; and,

     - To assist with design, requirements, and implementation of the FY 2006 TSGP.

   - Hiring of full-time or part-time staff or contractors/consultants and expenses related to:

     - Pre-application submission management activities and application requirements; and,

     - Meeting compliance with reporting/data collection requirements, including data calls.

   - Development of operating plans for information collection and processing necessary to respond to DHS/G&T data calls;

   - Travel expenses;

   - Meeting-related expenses (For a complete list of allowable meeting-related expenses, please review the OGO *Financial Management Guide* at http://www.dhs.gov/dhspublic/display?theme=18&content=4206); and,

   - Acquisition of authorized office equipment, including personal computers, laptop computers, printers and LCD projectors.

7. **Unauthorized Program Expenditures.** FY 2006 TSGP funds may not be used for the following activities:

   - Ferry systems participating in the FY 2006 TSGP cannot apply for projects already under consideration for FY 2006 Port Security Grant Program (PSGP) funding;
   - 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 or response functions), general-use vehicles, licensing fees, weapons systems and ammunition;
   - Personnel costs (except as detailed above);
   - Activities unrelated to the completion and implementation of the TSGP; and,
   - Other items not in accordance with the AEL or previously listed as allowable costs.

8. Specific Guidance on Canines

Eligible Costs: Eligible costs include the purchasing, training and certification of canines; all medical costs associated with initial procurement of canines; kennel cages used for transportation of the canines and other incidentals associated with outfitting and set-up of canines (such as leashes, collars, initial health costs and shots etc.). Eligible costs also include initial training and certification of handlers.

Ineligible Costs: Ineligible costs include but are not limited to hiring, costs associated with handler annual salary, travel and lodging associated with training and certification; meals and incidentals associated with travel for initial certification; vehicles used solely to transport canines; and maintenance / recurring expenses such as annual medical exams, canine food costs, etc.

Certification: Canines used to detect explosives must be certified by an appropriate, qualified organization. Such canines should receive an initial basic training course and also weekly maintenance training sessions thereafter to maintain the certification. The basic training averages 10 weeks for the canine team (handler and canine together) with weekly training and daily exercising. Comparable training and certification standards, such as those promulgated by the TSA Explosive Detection Canine Program, the National Police Canine Association (NPCA), the United States Police Canine Association (USPCA) or the International Explosive Detection Dog Association (IEDDA) may be used to meet this requirement[3].

[3] Training and certification information can be found at: http://www.tsa.gov/public/display?theme=32, http://www.npca.net, http://www.uspcak9.com/html/home.shtml, and http://www.bombdog.org/.

APPENDIX B

MASTER LIST OF RTSWGs AND REQUIRED PARTICIPANTS

Master List of RTSWGs and Required Participants

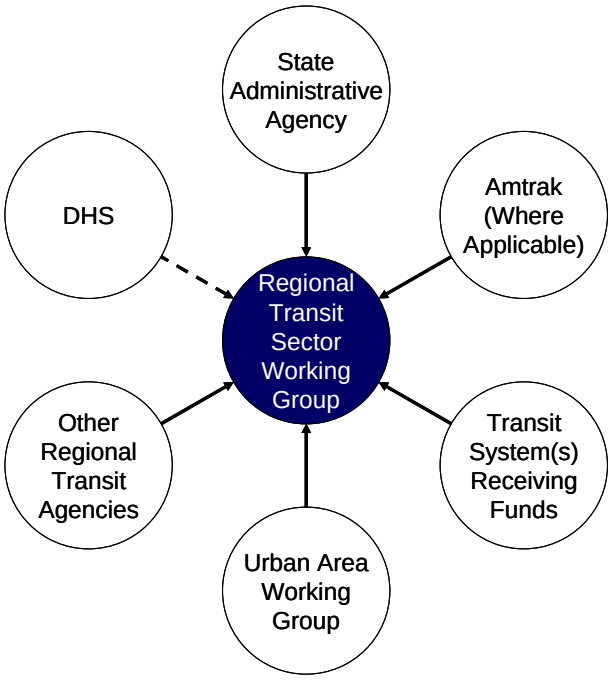
A. Purpose, Role and Composition of the RTSWG

The FY 2006 TSGP includes an optional requirement that transit systems eligible for funding participate in an RTSWG for the purpose of aligning the RTSS with the Goal and National Priorities..

In addition to the eligible transit systems, the RTSWG must also include representation from the applicable SAA(s) and Urban Area Working Group(s) (UAWG), and it is strongly recommended that other transit agencies whose systems intersect with those of the grant recipients also participate in the RTSWG process. In addition, where transit operations intersect with those of Amtrak in the National Capitol Region, Philadelphia, New York, Boston, Chicago, Seattle, Sacramento, Oakland, San Jose, Los Angeles and San Diego, a representative of Amtrak must be included in the RTSWG and close coordination on the expenditure of funds for security enhancements at shared facilities must occur. RTSWGs should also consider including representatives from existing Metropolitan Planning Organizations (MPOs) and Law Enforcement Planning Commissions (LEPCs), where feasible.

It is the responsibility of the applicable SAA(s) to coordinate and manage this process, and to ensure that updates to the RTSS are conducted in accordance with the guidance provided in this application kit.

The Regional Transit Security Working Group



B. Master List of RTSWGs and Required Participants

State SAA	RTSWG	Transit System	Other Participants
AZ	Phoenix	Regional Public Transportation Authority	
		City of Phoenix Public Transit Department	
CA	Los Angeles/Long Beach	Southern CA Regional Rail Authority	Amtrak
		LA County Metro Transp. Authority	
		City of Los Angeles Department of Transportation	
		Orange County Transportation Authority	
		Foothill Transit	
		Santa Monica's Big Blue Bus	
		Long Beach Transit	
	Bay Area	Peninsula Corridor Joint Powers Board	Amtrak
		SF Bay Area Rapid Transit District	
		Altamont Commuter Express Authority	
		Santa Clara Valley Trans Authority	
		San Francisco Municipal Railway	
		San Francisco Bay Municipal Transp. Authority	
		AC Transit	
		Central Contra Costa Transit Authority	
		San Mateo County Transit Authority	
		Caltrans Transbay Bus Terminal	
		Golden Gate Bridge, Highway and Transportation District	
		Blue & Gold Fleet (City of Alameda Ferry Services)	
		City of Vallejo Transportation Program	
	Sacramento	Sacramento Regional Transit District	Amtrak
	San Diego	North San Diego County Transit District	Amtrak
		San Diego Trolley	
		San Diego Metro Transit System	
CO	Denver	Regional Transportation District	
DC/MD/VA[4]	National Capital Region	Washington Metropolitan Area Transit Authority	Amtrak
		Maryland Transit Administration	
		VA Railway Express	
		Montgomery County Dept. of Transportation	
		Prince George's County Dept. of Public Works & Transportation	
		City of Alexandria – Alexandria Transit Co.	
		Fairfax County Dept. of Transportation	
		Potomac & Rappahannock Transportation Commission	

[4] The DC SAA will submit the RTSS, Investment Justification and Regional Transit Sector Overview on behalf of the RTSWG

State SAA	RTSWG	Transit System	Other Participants
FL	Jacksonville	Jacksonville Transportation Authority	
	Miami/Fort Lauderdale	Tri-County Commuter Rail	
		Miami-Dade Transit Agency	
		Broward County Division of Mass Transit	
GA	Atlanta	Metropolitan Atlanta Rapid Transit Authority	
		Georgia Regional Transportation Authority	
HI	Honolulu	City & County of Honolulu DOT Services	
IL/IN[5]	Chicago	NE Ill Reg Commuter Rail	Amtrak
		PACE Suburban Bus	
		No. Indiana Commuter Trans Dist	
		Chicago Transit Authority	
LA	New Orleans	New Orleans Regional Transit Authority	
		Jefferson Parish Department of Transportation	
		Louisiana Department of Transportation – Crescent City Connection	
MA	Boston	Massachusetts Bay Transportation Authority	Amtrak
MI	Detroit	Detroit Transportation Corp	
		Suburban Mobility Authority for Regional Transportation	
MN	Twin Cities	Metro Transit	
MO	Saint Louis	Bi-State Development Agency	
		Madison County Transit District (IL)	
NV	Las Vegas	Regional Transportation Commission of Southern NV	
NY	Buffalo	Niagara Frontier Transp. Authority	
NY/NJ/CT[6]	New York City Jersey City Newark	Metropolitan Transportation Authority	Amtrak
		Port Authority of New York and New Jersey	
		Westchester County Department of Transportation	
		New Jersey Transit Corporation	
		CT Department of Transportation	
OH	Cleveland	Greater Cleveland Regional Trans Auth	
	Cincinnati	Southwest Ohio Regional Transit Authority	
		Transit Authority of Northern KY	
OR	Portland	Tri-County Metropolitan Transportation District	
		Clark County Public Transp. Benefit Area Auth. Corp.	

[5] The IL SAA will submit the RTSS, IJ and Regional Transit Sector Overview on behalf of the RTSWG
[6] The NY SAA will submit the RTSS, IJ and Regional Transit Sector Overview on behalf of the RTSWG

State SAA	RTSWG	Transit System	Other Participants
PA	Pittsburgh	Cambria County Transit Authority	
		Port Authority of Allegheny County	
PA/NJ[7]	Philadelphia	PA Department of Transportation	Amtrak
		Port Authority Transit Corporation	
		Southeastern Pennsylvania Transportation Authority	
		New Jersey Transit Corporation	
TN	Memphis	Memphis Area Transit Authority	
TX	Dallas/Forth Worth/Arlington	Dallas Area Rapid Transit	
		Trinity Railway Express	
		Ft. Worth Transportation Authority	
	Houston	Island Transit	
		TX Dept. of Transportation (Bolivar Roads Ferry)	
		Metropolitan Transit Authority of Harris County	
	San Antonio	VIA Metro Transit	
WA	Seattle	Central Puget Sound Regional Trans Authority	Amtrak
		King County Dept of Transportation	
		Pierce County Public Transportation Benefit Area Authority Corporation	
		Snohomish County Public Transportation Benefit Area Authority Corporation	
		Washington State Ferries	
WI	Milwaukee	Milwaukee County Transit System	

[7] The PA SAA will submit the RTSS, IJ and Regional Transit Sector Overview on behalf of the RTSWG

APPENDIX C

REGIONAL TRANSIT SECTOR OVERVIEW GUIDANCE

Regional Transit Sector Overview Guidance

A. Overview of Requirements

The optional Regional Transit Sector Overview attachment must not exceed 5 pages. The format below is strongly suggested for this file attachment.

1. Transit Agency Contacts (for each eligible transit system)

- Point of contact's (POC) name and title;
- POC's full mailing address;
- POC's telephone number;
- POC's fax number;
- POC's email address;
- Also include the corresponding information for the single authorizing official for your organization—i.e., the individual authorized to sign a cooperative agreement award.

2. Description of Each Eligible Transit Agency's Operating System

- Infrastructure;
- Ridership data;
- Number of passenger miles;
- Number of vehicles and/or vessels;
- Types of service and other important features;
- System map;
- Geographical borders of the system and the cities and counties served;
- Other sources of funding being leveraged for security enhancements.

3. IED and CBRN Prevention, Detection and Response Capabilities

- Discuss the transit sector's ***current*** efforts to protect any underwater tunnel infrastructure from attacks involving IEDs:
  - Specific attention should be paid to any enhancements achieved as a result of FY 2005 TSGP funding;
- Discuss the transit sector's ***current*** prevention, detection and response capabilities relative to IEDs and CBRN devices generally (including sensors, canine units, etc.):
  - Specific attention should be paid to any enhancements in these capabilities achieved as a result of FY 2005 TSGP funding;
- Discuss the transit sector's ***current*** additional high consequence risk mitigation efforts, training programs for employees, emergency drills and citizen awareness activities:
  - Specific attention should be paid to any enhancements in these capabilities achieved as a result of FY 2005 TSGP funding;

- Discuss the transit sector's ***requirements*** relative to protection of any underwater tunnel infrastructure from attacks involving IEDs;
- Discuss the transit sector's ***required*** prevention, detection and response capabilities relative to IEDs and CBRN devices (including sensors, canine units, etc.);
- Discuss the transit sector's ***required*** high consequence risk mitigation needs, anti-terrorism training programs for employees, emergency drills and citizen awareness activities.

B. Submitting the Regional Transit Sector Overview

Release of funding is contingent upon the completion and submission of the Regional Transit Sector Overview. Awards will be special conditioned to prohibit obligation, expenditure and draw down of funds until a copy of Regional Transit Sector Overview is received and approved by DHS. ***Regional Transit Sector Overviews must be completed and submitted to G&T, along with the updated RTSS and Funding Justifications, within 90 days of the FY2006 TSGP regional award date..*** An electronic copy of the Regional Transit Sector Overview must be provided by the applicable SAA via the G&T secure portal at: https://odp.esportals.com/.

Important Note: Questions regarding the Regional Transit Sector Overview should be directed to your G&T Program Manager, or to the G&T Centralized Scheduling and Information Desk (CSID). The CSID can be contacted at 1-800-368-6498 or askcsid@dhs.gov. CSID hours of operation are from 8:00 a.m. to 7:00 p.m. (EST), Monday through Friday.

APPENDIX D

REGIONAL TRANSIT SECURITY STRATEGY GUIDANCE

Regional Transit Security Strategy Guidance

A. Overview of Requirements

Strategic planning, at its core, is a process that should guide the RTSWGs in achieving their goals and objectives. The current strategies have strong foundations that should support an ongoing process of review and refinement as new lessons are learned, new priorities are realized, and new homeland security guidance is released. With the release of the National Preparedness Goal and Guidance, RTSWGs have an opportunity to address the four core mission areas and reflect the National Priorities in their strategies.

Although DHS is requiring RTSWGs to revisit their current strategies, the intent of this guidance is not to require that an entirely new strategy be written, but rather to tailor and update, as appropriate, existing goals and objectives to support the National Preparedness Goal and the National Priorities. States and urban areas recently completed a similar process of alignment for their strategies. The changes required as part of the FY 2006 TSGP, will ensure that each RTSS remains consistent with the associated state and urban area strategies and will promote and allow for further integration of these planning efforts.

If desired, RTSWGs may conduct a more extensive update or rewrite of their strategies. However, at a minimum, RTSWGs must ensure that their updated strategies address the four mission areas (prevent, protect, respond, recover) and reflect the National Priorities[8]. It is important to note that it is not a requirement to provide an individual goal and objective for each National Priority and Action Item; RTSWGs must show, however, how their goals and objectives align to these priorities.

As part of this effort, RTSWGs must also review the RTSS to ensure it adequately addresses the following priorities specific to transit security: 1) the protection of any underwater tunnels from IED attacks; 2) prevention and detection capabilities for IEDs and other non-conventional weapons generally; 3) other high consequence risks identified through system-wide risk assessments; 4) anti-terrorism training for transit employees; 5) emergency drills; and, 6) citizen awareness activities. RTSWGs must also ensure that each RTSS continues to align with the goals and objectives contained within the relevant state and urban area strategy(ies).

It is recognized that each region has unique needs and capabilities, and the strategies should reflect these attributes. Therefore, strategies should continue to include additional goals and objectives that also reflect specific regional priorities.

[8] This does not require an update to existing objectives if those objectives already reflect the National Priorities. However, the alignment of those objectives to the National Priorities should be clearly articulated.

The current strategies, developed in FY 2005, are mostly terrorism focused. In updating their strategies this year, RTSWGs should begin the process of evolving their strategies to address not only terrorism, but a broad range of other threats and hazards, founded on a capabilities-based planning approach. In the future, states, urban areas and RTSWGs will be asked to develop enterprise-wide homeland security strategies for 2007, 2008 and 2009 that reflect the necessary integration and collaboration across all mission areas and support the establishment of the National Preparedness System and realization of the Goal.

B. Incorporating the National Priorities

The following paragraphs provide guidance on how to apply each of the relevant National Priorities to the RTSS.

1. How to apply the Expanded Regional Collaboration Priority to the FY 2006 RTSS Update

Preventing, protecting against, responding to, and recovering from major events (as represented by the National Planning Scenarios) will require that capabilities be drawn from a wide area. The area from which resources will be drawn may or may not expand beyond the transit sector served by the existing RTSWG. In updating their homeland security strategies, RTSWGs are asked to examine current regional collaboration efforts and explore new approaches to developing regional capabilities. The strategy should provide a narrative description of how the RTSWG currently uses and plans to use mutual aid to prevent, protect against, respond to, and recover from major events. The strategy should present the RTSWG's vision for increasing existing collaboration efforts and establishing and enhancing integrated regional operations for all mission areas.

In developing this vision and updating their strategies, RTSWGs should complete the following activities:

- ***Define current collaboration efforts already undertaken across the transit sector, across jurisdictions and across disciplines;***
- ***Discuss opportunities for future collaboration that can enhance capability within the region;***
- ***Define future goals and objectives for a regional approach for prevention, protection, response, and recovery;***
- ***Outline a process for integrating operational systems from multiple disciplines and jurisdictions for all mission areas.***

It is important to note that regional collaboration is not necessarily a structured, institutionalized program across a region, but better defined as a strategic vision for the future, with a multi-jurisdictional and multi-disciplinary approach to homeland security. There is not a one-size-fits-all approach to regional collaboration, but the RTSWG's vision should support an enterprise-wide approach to building capability for all the mission areas.

2. How to apply the Implement the National Incident Management System (NIMS) and National Response Plan (NRP) Priority to the FY 2006 RTSS Update

Both the NIMS and the NRP were formally issued by DHS after the initial strategies were submitted to G&T. As such, RTSWGs are being asked to show how their strategic goals and objectives support the implementation of NIMS and the alignment of their operational plans to the NRP; the updated strategies are not, however, intended to reproduce a completed NIMS implementation plan.

Updated strategies should indicate how RTSWGs will incorporate the NIMS/NRP into their emergency response plans, policies and procedures, incident and resource management, trainings, programs, and exercises. Strategies also should reflect how NIMS/NRP will support integrated regional operational systems. This will be part of the consistent nationwide approach for Federal, state, local, and tribal governments, as well as the private sector, to work together more effectively and efficiently to prevent, protect against, respond to, and recover from domestic incidents, regardless of cause, size, or complexity.

For further information on this priority:

- The NIMS can be found online at: http://www.fema.gov/pdf/nims/nims_doc_full.pdf
- The NRP can be found online at: http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf
- Additional information can be found online at: http://www.fema.gov/nims/

3. How to apply the Implement the Interim National Infrastructure Protection Plan (NIPP) Priority to the FY 2006 RTSS Update

Consistent with HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection," the NIPP reflects the 17 individual CI/KR sectors identified in the table on the next page.

Critical Infrastructure and Key Resource Sectors

Critical Infrastructure and Key Resource Sectors
Agriculture and Food
Public Health and Health Care
Drinking Water and Wastewater Treatment Systems
Energy
Banking and Finance
National Monuments and Icons
Defense Industrial Base
Information Technology
Telecommunications
Chemical
Transportation Systems
Emergency Services
Postal and Shipping
Dams
Government Facilities
Commercial Facilities
Nuclear Reactors, Materials, and Waste

As part of the FY 2006 TSGP, RTSWGs should work with the applicable states and urban areas to develop and implement a critical infrastructure protection program as a component of the overarching homeland security program for the region. This program should engage all relevant intergovernmental coordination points (e.g., Federal, state, local, and tribal) to ensure a comprehensive approach to critical infrastructure protection across all appropriate levels of government, across both public and private sectors, within geospatial areas, and across infrastructure sectors.

In updating their strategies, RTSWGs should provide a strategic context and vision for their infrastructure protection programs. In developing this vision, RTSWGs should consider how they will fulfill the following roles:

- Build a critical infrastructure protection program that implements the risk management framework outlined in the Interim NIPP. Chapter 3 of the Interim NIPP provides more detailed discussion of 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 not on the Federal list, but which are of concern to the region;
- Incorporate cyber security protection efforts across all sectors of CI/KR.

DHS is currently working in conjunction with Federal, state, local, tribal, and private sector stakeholders to update and finalize the NIPP.

For further information on this priority:

- Refer to the NIPP or send comments and questions to NIPP@dhs.gov
- The Department of Homeland Security's National Strategy for the Physical Protection of Critical Infrastructures and Key Assets: http://www.whitehouse.gov/pcipb/physical.html
- Homeland Security Presidential Directive – 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection": http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html
- The USA PATRIOT Act defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters.": http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107
- The President's *National Strategy for Homeland Security* (NSHS), issued in July 2002, restates the definition of critical infrastructure provided in the USA PATRIOT Act. The Strategy expands on this definition, however, summarizing its rationale for classifying specific infrastructure sectors as critical: http://www.whitehouse.gov/homeland/book/

4. How to apply the Strengthen Information Sharing and Collaboration Capabilities Priority to the FY 2006 RTSS Update

RTSWGs are encouraged to develop a strategic framework that outlines an overall vision and approach relative to the *Information Sharing and Collaboration Priority*. For the RTSSs, consideration should be given to how the fusion process will be established, i.e., as a stand-alone capacity or through direct integration into a statewide or regional structure, as well as how it will be organized and coordinated.

Some goals to consider in the development of the strategic framework include:

- Ensuring that the fusion process is fully capable of communicating effectively and efficiently with the Federal Government through the Homeland Security Information Network (HSIN), the Homeland Security Operations Center (HSOC), 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 HSOC, 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, 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 is essential.

For further information on this priority:

The Global Justice Information Sharing Initiative will release the 'Recommended Minimum Standards for Establishing and Operating the Intelligence Component of Fusion Centers for Local, State, Tribal, and Federal Law Enforcement,' in the ensuing months.

Information Sharing and Collaboration information can be found at the following web sites:

- DHS Homeland Security Information Network (HSIN) website: http://www.dhs.gov/dhspublic/display?theme=43&content=3747&print=true
- Southwest Emergency Response Network website: www.swern.gov
- NorthWest Warning, Alert & Response Network website: www.nwwarn.gov
- Homeland Security Advisory Council Intelligence and Information Sharing Initiative: http://www.dhs.gov/interweb/assetlibrary/HSAC_IntelInfoSharingReport_1204.pdf

  Information on FBI and related DOJ efforts in this area can be found at: http://www.fbi.gov/terrorinfo/counterrorism/waronterrorhome.htm

5. How to apply the Strengthen Interoperable Communications Capabilities Priority to the FY 2006 RTSS Update

RTSWGs should show in their updated strategy how they plan to support regional interoperability. The strategy should also illustrate how the process is to be implemented using the five elements within the Interoperability Continuum, and clearly explain how the interoperable communication goal(s) fits into the overall framework of the Continuum.

For further information on this priority:

- For information on G&T's Interoperable Communications Technical Assistance Program (ICTAP): *http://www.ojp.usdoj.gov/odp/ta_ictap.htm*

- More information on implementing interoperable communications can be obtained from SAFECOM at: http://www.safecomprogram.gov/SAFECOM/grant/default.htm

- SAFECOM grant guidance can be found at: http://www.safecomprogram.gov/SAFECOM/grant/default.htm

APPENDIX E

THE FTA TOP 20 SECURITY PROGRAM ACTION ITEMS

The FTA Top 20 Security Program Action Items

TOP 20 SELF-ASSESSMENT CHECKLIST

FTA Top 20 Security Program Action Items for Transit Agencies: Self-Assessment Checklist

I. Management and Accountability

1. Written security program and emergency management plans are established.

Baseline Practices:

- ❑ Does a System Security Plan exist?
- ❑ Does an Emergency Management Plan exist?
- ❑ Do standard and emergency operations procedures (SOPs/EOPs) for each mode operated, including operations control centers, exist?

Exemplary Practices:

- ❑ *Do Continuity of Operations Plans exist?*
- ❑ *Does a Business Recovery Plan (administration, computer systems, operations, etc.) exist?*

2. The security and emergency management plans are updated to reflect anti-terrorist measures and any current threat conditions.

Baseline Practices:

- ❑ What is the date of the latest update?
- ❑ Are security plans reviewed at least annually?
- ❑ Are reviews and changes to the plans documented?
- ❑ Does the plan now include weapons of mass destruction protocols?

3. The security and emergency management plans are an integrated system security program, including regional coordination with other agencies, security design criteria in procurements and organizational charts for incident command and management systems.

Baseline Practices:

- ❑ Are emergency management plans integrated with the regional emergency management authority plans?
- ❑ Do management & staff participate in planning and conducting emergency security activities (e.g., drills, committees, etc.)?
- ❑ Does management coordinate with the FTA regional office?
- ❑ Are mutual aid agreements with other regional public agencies (e.g., local government, fire, police, other transit agencies, etc.) approved and signed?
- ❑ Does an inter-departmental program review committee exist and address security issues?

Exemplary Practice:
❑ *Is security design criteria/Crime Prevention Through Environmental Design (CPTED) included in system security program plan?*

4. The security and emergency management plans are signed, endorsed and approved by top management.

Baseline Practices:
❑ Is there a policy statement emphasizing the importance of the security plan?
❑ Is the security plan approved and signed by the top official?

5. The security and emergency management programs are assigned to a senior level manager.

Baseline Practices:
❑ What are the name and title of the security program manager?
❑ Is there a current organizational chart identifying the reporting structure for the security program manager?

6. Security responsibilities are defined and delegated from management through to the front line employees.

Baseline Practices:
❑ Are security plans distributed to appropriate departments in the organization?
❑ Do regular senior and middle management security coordinating meetings occur?
❑ Do informational briefings occur whenever security protocols are substantially updated?
❑ Are lines of delegated authority/succession of security responsibilities established and known?

7. All operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control.

Baseline Practices:
❑ Are regular supervisor and foreperson security review & coordinating briefings held?
❑ Does a security breach reporting system exist and are reports addressed through the security program review committee?
❑ Is facility security (e.g., perimeter/access control) supervision compliance monitored on a regular basis?

II. Security Problem Identification

8. A threat and vulnerability assessment resolution process is established and used.

Baseline Practices:
❑ Does a threat and vulnerability process exist and is it documented?
❑ Is a threat and vulnerability assessment conducted whenever a new asset/facility is added to the system?

❑ Have management & staff responsible for managing the threat and vulnerability assessment process received adequate training?
❑ Is the threat and vulnerability process used to prioritize security investments?

9. Security sensitive intelligence information sharing is improved by joining the FBI Joint Terrorism Task Force (JTTF) or other regional anti-terrorism task force; the Surface Transportation Intelligence Sharing & Analysis Center (ISAC); and security information is reported through the National Transit Database (NTD).

Baseline Practices:
❑ Does the transit agency participate in its region's JTTF or coordinate with key police and intelligence agencies?
❑ Has the transit agency joined the ST-ISAC?
❑ Does the transit agency provide security information to the National Transit Database?

III. Employee Selection

10. Background investigations are conducted on all new front-line operations and maintenance employees (i.e., criminal history and motor vehicle records).

Baseline Practices:
❑ Are background checks conducted consistent with state and local laws?
❑ Is the background investigation process documented?

11. Criteria for background investigations are established.

Baseline Practice:
❑ Are the criteria for background checks by employee type (operator, maintenance, safety/security sensitive, contractor, etc.) documented?

IV. Training

12. Security orientation or awareness materials are provided to all front-line employees.

Baseline Practices:
❑ Are security orientation and awareness training materials updated to include counter-terrorism/WMD information?
❑ Is there a system in place to track who received what training when?

Exemplary Practice:
❑ *Are security awareness pocket guides distributed to all front-line employees?*

13. Ongoing training programs on safety, security and emergency procedures by work area are provided.

Baseline Practices:
❑ Are training programs, materials and informational briefings tailored to specific work

groups' activities?
❑ Are training program campaigns held whenever there are substantial updates to security and emergency management plans?

14. Public awareness materials are developed and distributed on a system wide basis.

Baseline Practice:
❑ Are security awareness print materials prominently displayed throughout the system (e.g., channel cards, posters, fliers, etc.)?
❑ Is the transit agency participating in the industry's Transit Watch program?

V. Audits and Drills

15. Periodic audits of security policies and procedures are conducted.

Baseline Practices:
❑ Are audits conducted periodically?
❑ Is there a disposition process for handling the findings and recommendations from the audits?

16. Tabletop and functional drills are conducted at least once every six months and full-scale exercises, coordinated with regional emergency response providers, are performed at least annually.

Baseline Practices:
❑ Are tabletop exercises conducted at least every six months?
❑ Does the agency participate in full-scale, regional field drills, held at least annually?
❑ Are tabletop and drill de-briefings conducted?
❑ Are after-action reports produced and reviewed for all tabletop exercises and field drills?
❑ Are plans, protocols and processes updated to reflect after-action report recommendations/findings?

VI. Document Control

17. Access to documents of security critical systems and facilities are controlled.

Baseline Practice:
❑ Have security critical systems, such as tunnel HVAC systems and intrusion alarm detection systems, been identified and documented?

Exemplary Practices:
❑ *Is access to security critical systems' documents controlled?*
❑ *Is there an identified department/person responsible for administering the policy?*
❑ *Do regular security committee meetings/briefings include reviewing document control compliance issues?*

18. Access to security sensitive documents is controlled.
Baseline Practice:
❑ Have sensitive security information (SSI) documents, such as security plans and protocols, been identified?

Exemplary Practices:
❑ *Is there a documented policy for designating and properly handling SSI documents?*
❑ *Do regular security committee meetings/briefings include reviews of SSI related matters?*

VII. Access Control

19. Background investigations are conducted of contractors or others who require access to security critical facilities, and ID badges are used for all visitors, employees and contractors to control access to key critical facilities.
Baseline Practices:
❑ Have security critical facilities been identified?
❑ Is the contractor background investigation process documented?
❑ Is the quality control of the process monitored on a regular basis?
❑ Are the criteria for contractor background checks documented?
❑ Are ID badges used for employee access control? (both policy and actual practice)
❑ Are ID badges used for visitors and contractors? (both policy and actual practice)
❑ Have security critical facilities been identified?
❑ Are there documented policies for restricting access to security critical facilities?

VIII. Homeland Security

20. Protocols have been established to respond to the Office of Homeland Security Threat Advisory Levels.

Baseline Practices:
❑ HSAS threat advisory levels process integrated into security plans and standard/emergency operating procedures
❑ Are specific protective measures defined and developed?

Notes:
(1) This checklist covers all modes directly operated by the transit agency (e.g., bus, light rail, heavy rail, etc.), and under contract operation (e.g., paratransit, fixed route bus, vanpools, etc.).
(2) Baseline Practices are considered the minimum requirements needed to meet the overall security action item; Exemplary practices are additional/supplemental activities associated with exceeding the minimum requirements and are candidates for industry best practices.
(3) Additional informational resources/references are available at "FTA Top 20 Security Program Action Items for Transit Agencies" website:
http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/Top20

(4) Questions? Please contact Rick Gerhart, FTA Office of Safety and Security at (202) 366-8970 or Richard.Gerhart@fta.dot.gov November 7, 2003

APPENDIX F

NATIONAL ENVIRONMENTAL POLICY ACT GUIDANCE

National Environmental Policy Act Guidance

The National Environmental Policy Act, 42 USC§§4321-4370d (NEPA) requires, among other things, that Federal agencies consider the environmental impacts of any major Federal action. In order to implement NEPA and its associated regulations, the Office of Grants and Training (G&T) requires Applicants, pursuant to the Assurances related to this grant program, to submit responses to questions regarding the Applicant's proposed project. Applicants are required to submit a brief explanation supporting each response of "yes" or "no". Applicants with multiple projects must submit separate responses for each project, and should consider the cumulative impact of the projects.

Federal agencies may establish categories of actions that, based on experience, do not individually or cumulatively have a significant impact on the human environment and, therefore, can be excluded from NEPA requirements to prepare an Environmental Assessment or Environmental Impact Statement. G&T has adopted certain such Categorical Exclusions. These Categorical Exclusions, however, only apply when the entire action fits within the exclusion, the action has not been segmented, and there are no extraordinary circumstances with the potential for significant impacts relating to the proposed action. The purpose of the questionnaire is to collect information from which a decision can be made whether application of a categorical exclusion is appropriate and whether further environmental analysis is required.

If, in the course of responding to the questions, the Applicant concludes that an Environmental Assessment (EA) under NEPA may be required for the proposed project, the Applicant should submit such EA in conjunction with the responses to the questions, or as soon thereafter as possible. G&T will not issue an award until after NEPA compliance has been completed. G&T may independently conclude, based on its review of the responses to the questions, that an EA is required and will contact the Applicant to notify it of that requirement. Submission of an EA prior to G&T request will eliminate any associated delay in review prior to issuance of an award.

Requirements on the contents of an EA can be found in regulations promulgated by the Council on Environmental Quality (CEQ) at 40 CFR Part 1508.9 (and may be found on the web at http://ceq.eh.doe.gov/nepa/regs/ceq/toc_ceq.htm). Note that 40 CFR §1508.9 indicates that the EA is a concise document. It is G&T's intention to adhere to this instruction and to require only enough analysis to accomplish the objectives specified by the regulations.

This information may be provided using one of the attachment fields within Grants.gov.

Transit Security Grant Program
NEPA Resource Guide

Applicant Name:
Application Number:

Question 1: Is the project likely to have a significant impact on properties protected under section 106 of the Historic Preservation Act of 1966, as amended (16 USC§470), E.O. 11593 (identification and protection of historic properties), and the Archaeological and Historic Preservation Act of 1974 (16 USC §§469a-1 et. seq.)?

Examples

For example, will historic buildings or archeological sites be affected by the project?

Helpful Links

Historic Preservation Act of 1966, as amended (16 USC§470)
http://www4.law.cornell.edu/uscode/16/470.html

Executive Order 11593 (identification and protection of historic properties)
http://gsa.gov/Portal/gsa/ep/contentView.do?P=XAE&contentId=12094&contentType=GSA_BASIC

Archaeological and Historic Preservation Act of 1974 (16 USC §§469a-1 et. seq.)
http://www4.law.cornell.edu/uscode/16/469a-1.html

National Register of Historic Places
http://www.cr.nps.gov/nr/

Question 2: Is the project likely to be highly controversial on environmental grounds? The project is considered highly controversial when it is opposed on environmental grounds by a Federal, state, or local government agency or by a substantial number of persons affected by the project.

Examples

Have you had any Federal, state, or local government opposition to past projects? Are there community advocacy or homeowners groups near your facility that may oppose the project?

Question 3: Is the project likely to have a significant impact on natural, ecological, cultural, or scenic resources of national, state, or local significance?

Examples

For example, are there any vistas, landmarks, wetlands, or cultural resources (e.g., areas which have significant cultural importance to Native Americans) that may be affected by the project?

Question 4: Is the project likely to be highly controversial with respect to the availability of adequate relocation housing? In a project involving relocation of persons or businesses, a controversy over the amount of acquisition or relocation payments is not considered to be a controversy with respect to the availability of adequate relocation housing.
Examples *Will families or communities be displaced either for short or long term as a result of the project?*
Question 5: Is the project likely to cause substantial division or disruption of an established community, or disrupt orderly, planned development, or is it likely to not be reasonably consistent with plans or goals that have been adopted by the community in which the project is located?
Examples *For example, will the project result in road closures or fencing which could impact community accessibility?*
Question 6: Is the project likely to cause a significant increase in surface traffic congestion?
Examples *For example, would credential checks at gates or the closing of publicly accessible access roads result in congestion on public roads?*
Question 7: Is the project likely to have a significant impact on noise levels of noise sensitive areas?
Examples *For example, would the project create excessive noise resulting in discomfort, inconvenience, or interference with the use and enjoyment of property? Will the project have potential to result in the violation of local noise ordinances? Secondly, many National Parks are imposing restrictions to preserve the natural "soundscapes", or to protect wildlife that could be adversely affected.*
Question 8: Is the project likely to have a significant impact on air quality or violate the local, state or Federal standards for air quality?
Examples *Check with your state's Environmental Protection Agency, or some areas have local air quality boards or districts.*

Question 9: Is the project likely to have a significant impact on water quality or contaminate a public water supply system?

Examples

For example, would run off from construction, fencing or barriers affect surface water sources or local reservoirs?

Question 10: Is the project likely to be inconsistent with any Federal state, or local law or administrative determination relating to the environment?

Helpful Links

A good place to check would be your Regional Council of Government.
National Association of Regional Councils
http://www.narc.org/

Question 11: Is the project likely to directly or indirectly affect human beings by creating a significant impact on the environment?

Helpful Links

Definitions of significant impact can be found on the Council of Environmental Quality's website (Sec. 1508.27 Significantly).
http://ceq.eh.doe.gov/nepa/regs/ceq/1508.htm#1508.27

APPENDIX G

BIANNUAL STRATEGY IMPLEMENTATION REPORT GUIDANCE

Biannual Strategy Implementation Report Guidance

A. Biannual Strategy Implementation Report (BSIR) Web Application

G&T will provide a web application for submission of the BSIR. All reports must be completed and submitted to G&T electronically using the web application. All information submitted to G&T through these reports is considered to be dynamic. Each report submitted will be stored as a historical record of that submission. Updates will be made during subsequent submissions. It is therefore critical that each report submitted be comprehensive and include a thorough update of all information requested. All reports must be transmitted via the web in accordance with G&T-scheduled submission deadlines. The URL to the new web application is https://www.reporting.odp.dhs.gov/.

B. BSIR Report

For this grant process, applicants are not required to provide budget detail worksheets with their application. ***However, grantees will be required to submit budget data to G&T via the web as part of their June and December BSIR submissions. The BSIRs should account for all funds awarded, and the applicable SAAs are responsible for completing and submitting all BSIR reports to G&T.***

The BSIR is a detailed report of the planned activities associated with G&T grant funding. BSIR submissions are required to be completed biannually, and are due on July 31st and January 31st of each year. The BSIR will provide a complete accounting of how the state has complied with the requirement to pass through 97% of all funds to transit agencies, and will also demonstrate how the planned expenditure of grant funds will be used to administer the grant and to fund the critical resource gaps identified in the RTSS. This will be accomplished through the specific identification of a project or projects to be accomplished by each sub-grantee with funds provided during the grant award period. All funds provided must be linked to one or more projects. States are reminded to keep a record of sub-grantee budget worksheets and must make them available for DHS review upon request.

This report must be completed for all funds retained by the state and for each sub-award. Allocation of all financial resources provided through the FY 2006 TSGP must be used to fund the critical resource gaps identified in the RTSS.

C. Grant Reporting Timeline

Based on a 30 month period of performance, G&T expects most grants will have a reporting schedule similar to timeline below (see Figure 1). Most grants will have SEVEN submissions over the course of the period of performance including, ***six BSIR submissions, and one final BSIR submission.***

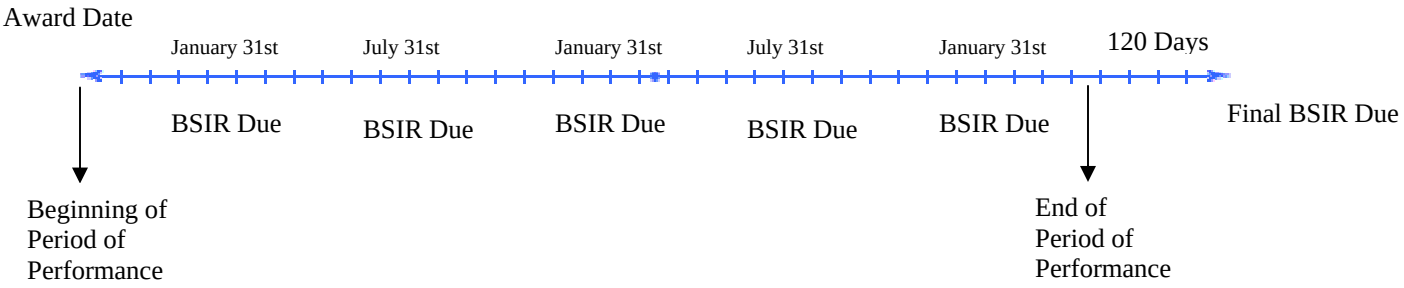


Figure 1. Grant Reporting Timeline

D. Reported Information

While the web application for the BSIR will be provided to grantees, it is important for applicants to fully understand the data points that must be collected. Each BSIR will include, but is not limited to, the following information for funds provided to each sub-grantee and funds retained at the state level:

1. Jurisdiction Name
2. Total Award Amount
3. List the oal or objective that is being supported by the project
4. Identify the amount of funding designated for each discipline from each grant program area:
   Identify the solution area(s) in which expenditures will be made and the amount that will be expended under each solution area:
   - Planning
   - Organization
   - Equipment
   - Training
   - Exercises
   - M&A
5. Metrics indicating project progress/success

Note: *The web application provided by G&T will include appropriate data fields for all information discussed above. Additionally, brief narrative descriptions may be required for certain data points, such as project titles, etc.*

APPENDIX H

APPLICATION CHECKLIST

Application Checklist

All G&T TSGP applicants must complete the following:

SF-424 Grant Application with Certifications (through Grants.gov)
- □ Non-Supplanting Certification
- □ Assurances
- □ Certifications Regarding Lobbying; Debarment, Suspension, and Other Responsibility Matters; and Drug-Free Workplace Requirement

□ **Regional Transit Sector Overview (optional)**
- □ See guidance in Appendix C
- □ Submit via secure portal at: https://odp.esportals.com/

□ **Revised Regional Transit Security Strategy (optional)**
- □ See guidance in Appendix D
- □ Submit via secure portal at: https://odp.esportals.com/

□ **NEPA Checklist for *each* project (as a file attachment in Grants.gov), if applicable**
- □ See form in Appendix F

□ **DUNS Number (through Grants.gov form)**

For New Transit Systems Only (those not eligible for TSGP funding in FY 2005)

□ **Individual System Risk Assessment**
- □ Submit via secure portal at: https://odp.esportals.com/

□ **Individual Agency Security and Emergency Preparedness Plan**
- □ Submit via secure portal at: https://opd.esportals.com/

APPENDIX I

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 to our agency by the deadline specified. While your registration is pending, you may continue with steps 2, 3, and 4 of these instructions. Registration must be complete for you to be able to submit (step 5) and track (step 6) an application.

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, **97.075**. 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 J

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 Office of Grant Operations 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: Phone Activated Paperless System (PAPRS) and Letter of Credit Electronic Certification System (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 K

ADDITIONAL GUIDANCE ON THE NATIONAL PREPAREDNESS GOAL AND THE NATIONAL PRIORITIES

A. The National Preparedness Goal[9]

> ***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.[10] 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 National Response Plan (NRP), National Incident Management System (NIMS), and the National Infrastructure Protection Plan (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 1.

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

Figure 1. 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.

Appendix L provides guidance on how to utilize capabilities based planning to implement the National Preparedness Goal.

The Goal and the TCL are all-hazard 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 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.[11] 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.[12] 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.[13]

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 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

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

allowing appropriate citizen response.[14] 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.[15]

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.

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

[14] NIMS, March 2004.
[15] NIMS, March 2004.

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.[16] 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, critical infrastructure/key resource (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.

This *Program Guideline and Application Kit* implements the National Strategy for Transportation Security (NSTS) by addressing several key areas, including:

- Identification and evaluation of transportation assets;
- Fostering a risk-based approach;
- Validating appropriate and practical cost effective means of defending assets from attack;
- Assisting in the definition and management of roles and responsibilities between Federal, state, regional, local, and tribal authorities, as well as the private sector: and,
- Helping to understand the delineation of roles and responsibilities for Response and Recovery.

Alignment of planning efforts, funding requests, and project plans by eligible transportation sector applicants in response to this *Program Guideline and Application Kit* with the National Priorities and the TCL will further contribute toward efforts to implement the integrated, comprehensive approach to the protection of CI/KR envisioned by these grants.

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:

[16] 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.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 embracing 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.

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 evolving or potential Incidents of National Significance. 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 National Integration Center. The NIC web page, http://www.fema.gov/nims, is updated regularly with information about the NIMS and additional guidance for implementation.

Appendix M provides a copy of the NIMS Implementation Matrices.

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. 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 Transit Security Grant Program 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 CI/KR-related protection initiatives and programs within identified jurisdictions. Infrastructure protection programs include grants for specific activities that focus on the protection of CI/KR, such as ports, mass transit, rail transportation, etc. These funds support CI/KR protection capabilities based on risk and need in coordination with DHS, Sector-Specific Agencies (SSA), and Federal priorities.

The major goal for this priority in FY 2006 is the successful implementation of the NIPP. The NIPP was released in February 2005. The revised NIPP Base Plan is expected to be completed in 2006. It will detail milestones and implementation actions to:

- Establish the architecture for conducting risk assessment and risk management activities;
- Provide processes for coordinating resource priorities;
- Strengthen 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 will be delivered to DHS within 180 days of signature of the NIPP Base Plan. Implementing the NIPP and the Sector-Specific Plans (SSP) are important initial steps in achieving and sustaining many of the capabilities identified in the Goal and TCL. The DHS National Infrastructure Protection Plan 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. Chapter 3 of the NIPP provides 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 not on the Federal list, but which are 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.

Appendix N provides additional information on the NIPP and its relevance to the transportation sector.

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 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 Homeland Security Operations Center (HSOC) 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 the Homeland Security Information Network (HSIN), the HSOC, 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 HSOC), 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.

- 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.

Appendix O provides additional information on public safety communications and interoperability.

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.

Appendix P provides additional information on CBRNE threats and information on DNDO.

APPENDIX L

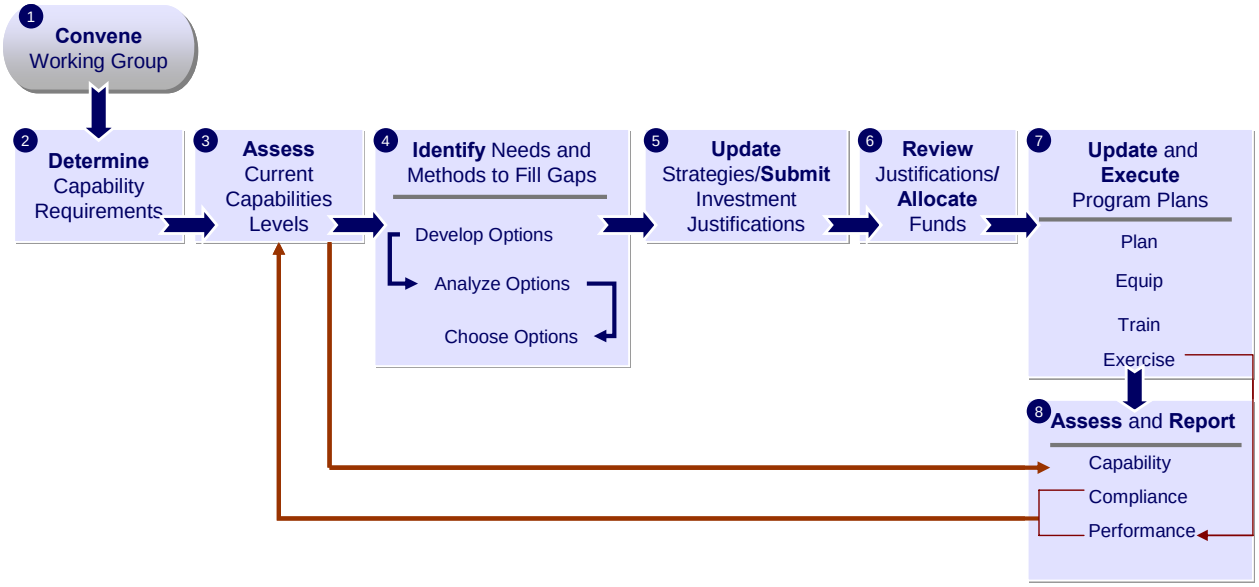
CAPABILITIES BASED PLANNING GUIDANCE

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.

Capabilities-Based Planning Process



Step 1: Convene a Working Group

For transit agencies this role could be filled by the RTSWG, the AMSC in port areas, or internal working groups.

Step 2: Determine Capability Requirements

The working group will determine risk-based target levels for each capability by reviewing the TCL and analyses of risk, threat, vulnerability and likelihood of occurrence. Such "target levels" should take into account current capabilities and resources, and a realistic appraisal of what additional resources may be available or appropriate for the particular jurisdiction.

The TCL provides a series of examples of how the 37 Capabilities may apply to jurisdictions of different sizes. These examples are intended to provide guidance on how the target levels listed in the individual Capabilities will vary based on the region and implementing agency. The TCL is *not* intended to direct resource

requirements for every agency or jurisdiction for each year, nor is it descriptive of the resources necessary for every type of scenario.

Step 3: Assess Current Capability Levels

The core of the capabilities-based planning approach is the need to compare current capabilities with risk-based target levels. The working group will coordinate an assessment of current level of capability of the entities represented on the working group. Capability assessments measure current level of capability against the target levels of capability from the TCL applicable to the level of government. Comparison will reveal "gaps" (implying outcomes cannot be accomplished with current capabilities); "excesses" (unnecessary redundancy exists or a specific capability is no longer needed); and "deficiencies" (a capability exists, but is insufficient to provide a reasonable assurance of success against a specified scenario). All required capabilities and expertise will not be present in the state or jurisdiction. Many will be secured through multi-agency coordination (i.e., mutual aid, acquisition through contracting, and resources from non-governmental and private sector partners).

DHS is currently conducting a pilot project in coordination with other Federal departments and agencies to aid in the development of a standard methodology for capability assessments. More specific information will be provided in future year program guidance.

Step 4: Identify, Analyze and Choose Options

An important aspect of capabilities-based planning is in selecting methods to fill capability gaps and deficiencies. This step is involves translating a capability gap or deficiency into specific needs and determining a mix of resource needs. The approach involves an analytical process using comparative, trade-off, and risk analysis. Recognizing that there is usually more than one resource combination that can address a capability gap or deficiency, the analysis involves identifying options, analyzing options, and choosing options, using the recommended resources identified in the TCL as a guide. This analysis provides senior decision makers with alternative combinations of resources or solution sets for each capability gap or deficiency. The analysis components are described below:

- ***Identify Options –*** In identifying options, the range of options should be kept to a manageable number, but solutions should be framed in ways to implement a capability. In reviewing options, the effectiveness of applying mutual aid between geographic areas and levels of government should be considered. A capability may be delivered with any combination of properly planned, organized, equipped, trained and exercised personnel that achieve the desired outcome. These elements of capability are described in detail in the Figure on the next page.

Elements of Capability

Personnel	Paid and volunteer staff who meet relevant qualification and certification standards necessary to perform assigned missions and tasks.
Planning	Collection and analysis of intelligence and information, and 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.
Organization and Leadership	Individual teams, an overall organizational structure, and leadership at each level in the structure that comply with relevant laws, regulations, and guidance necessary to perform assigned missions and tasks.
Equipment and Systems	Major items of equipment, supplies, facilities, and systems that comply with relevant standards necessary to perform assigned missions and tasks.
Training	Content and methods of delivery that comply with relevant training standards necessary to perform assigned missions and tasks.
Exercises, Evaluations, and Corrective Actions	Exercises, self-assessments, peer-assessments, outside review, compliance monitoring, and actual major events that provide opportunities to demonstrate, evaluate, and improve the combined capability and interoperability of the other elements to perform assigned missions and tasks to standards necessary to achieve successful outcomes.

NOTE: Elements of capability are consistent with NIMS

- ***Analyze Options.*** Once a range of options are identified, each should be analyzed and prioritized against a standard set of criteria. The analysis will determine which combination of resources may provide the desired capability or capabilities and address risk appropriately. Examples of criteria include:

  - Ability of the identified approaches to provide the desired capability. It may not be required to invest in all six elements at one time in order to achieve a capability due to prior investments;

  - Ability of the approaches to deliver the total capability. If it cannot deliver the total capability, evaluate how much of the capability can be met;

  - Delivery time frame; and

  - Relative improvement in capability level provided by the approaches as compared to the existing capability; and cost to develop, procure and sustain the approaches versus the cost to sustain the existing capability.

- ***Choose Options.*** The results of the analysis are presented to senior decision makers for consideration. Risk determinations are embedded in the decision making process. Risk determinations will consider the range of capability gaps, excesses, and deficiencies; issues identified during analysis (as identified in the analyze options component criteria); strategic concerns and implications; and consider the following:

  - Can the capability outcome be accomplished and provide a reasonable assurance of success?
  - What are the potential costs as compared to other options? Are the costs appropriate for the benefit gained and does the timing impact results?
  - What is the impact on planning? Is the solution compatible with other solutions available through the same or different Federal assistance programs and can mutual aid be applied?

  By applying known constraints and examining all capabilities, a preferred solution set will be selected by conducting comparative, trade-off and risk analysis. The results will be consolidated into a prioritized, balanced, resource-constrained portfolio across all relevant capabilities.

The following steps (5-8) are focused toward state or regional planning groups or entities that currently have the ability to allocate funds based on regional preparedness strategies. However, the process will still provide valuable guidance on the identification of cost effective projects that address strategic preparedness goals and objectives.

Step 5: Update Strategies and Submit Funding Justifications

Once options are chosen, entities can update their preparedness strategies and prepare and submit annual Funding Justifications. The strategies should be aligned with the National Preparedness Goal, State and Urban Area Homeland Security Strategies, and support and facilitate cooperation and mutual aid. Strategies are multi-year planning vehicles supported by specific annual work plans that describe each year's approach to meeting the longer term strategy. Funding Justifications should identify prioritized resource needs to close capability gaps.

Step 6: Review Justifications and Allocate Funds

The review of Funding Justifications and allocation of funds occurs at all levels of government. At each level, relevant decision makers will lead a comparison of Funding Justifications and map these to current resources under their control or to potential sources of funding. Using capabilities-based planning, the aim is to produce an effective mixed preparedness portfolio across the Nation. Ultimately, balancing the Federal preparedness portfolio will contribute to a more prepared Nation through the following:

- Maximizing the allocation of national preparedness investments and resources in compliance with homeland security strategies and the National Preparedness Goal to improve preparedness in the most efficient and effective manner;
- Providing clarity in resource allocation decisions based on consistent criteria and decision-making framework; and,
- Encouraging a regional and/or mutual-aid partner approach to national preparedness.

Once funds are allocated, annual work plans may be updated to reflect the funding received and the associated courses of action to build capabilities in accordance with the overall guiding strategy.

Step 7: Update and Execute Program Plans

Execution is where the strategies and plans previously developed and/or updated are implemented. Annual work plans are carried out by all relevant stakeholders. Execution is focused on:

- Administering programs;
- Conducting planning and coordination;
- Purchasing equipment in accordance with documented needs and specified standards, as well as preparing and maintaining such equipment to be readily available as needed;
- Developing and conducting training to fill capability gaps; and,
- Developing and conducting exercises to demonstrate performance.

Step 8: Assess and Report

An assessment process provides a continuously validated baseline for preparedness levels. Capability, compliance, and performance assessments provide the basis to determine the preparedness of individual areas and levels of governments, as well as serve to view preparedness from a national perspective. Capability assessments are discussed in Step 3. Other types of assessment include performance and compliance assessments. Performance and compliance assessments serve to validate levels of capability. Compliance assessments will provide insight into conformance with requirements (e.g., NIMS and other national programs). Performance assessments will be provided through exercise program results.

Assessments should be performed on a regular basis. Data from assessments serve to update and validate the preparedness baseline. Information from these assessments provides a comprehensive indicator for how well capability levels are achieved and maintained. The results of these assessments will be presented to decision makers for discussion and will be used as a mechanism to develop subsequent guidance. Analysis from assessments will enable decision makers at all levels to ensure the appropriate balance among resources allocated to strengthen specific capabilities. This analysis will also help to develop a comprehensive “snapshot” of national preparedness. Overall

progress towards increasing our national level of preparedness will be documented and communicated through a national reporting cycle and Annual Status Report.

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 M

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 NIMS Integration Center (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. Homeland Security Presidential Directive 5 (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[17] 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[18] 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:

[17] 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)

[18] 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, 9-1-1 centers and multi-agency coordination systems such as Emergency Operations Centers (EOC).

How NIMS Applies to the Transportation Sector:

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

For example, the National Response Plan (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 Emergency Operations Plans (EOP);
- Promotion of intrastate mutual aid agreements;
- Coordinating and providing technical assistance to local entities regarding NIMS;
- Institutionalizing the use of the Incident Command System (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 National Response Plan (NRP), the Goal and the National Infrastructure Protection Plan (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.

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. • The NIMS Capability Assessment Support Tool (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.	• 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 • NIMS Capability Assessment Support Tool (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 • NIMS Capability Assessment Support Tool (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 (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 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 Emergency Operations Centers (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. The NIMS Capability Assessment Support Tool (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 • Catalog of Federal Domestic Preparedness Assistance (CFDA): http://www.cfda.gov	
Revise and update plans and SOPs to incorporate NIMS and National Response Plan (NRP) components, principles and policies, to include planning, training, response, exercises, equipment, evaluation and corrective actions	• National Response Plan (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. • Emergency Operations Plan (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 NIMS Integration Center (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 National Response Plan (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. • The Emergency Management Institute (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 National Incident Management System (NIMS). The NIMS is a comprehensive system that improves tribal and local response operations through the use of the Incident Command System (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. Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*, requires all Federal Departments and agencies to adopt and implement the NIMS, and requires state[19] and local[20] 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 local community or 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

[19] 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)

[20] 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)

- Establish communication processes, procedures and protocols that will ensure effective interoperable communications among emergency responders, 9-1-1 centers, and multi-agency coordination systems (Emergency Operations Centers).

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 NIMS Integration Center (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, the National Incident Management Capability Assessment Support Tool (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 National Response Plan (NRP), the Homeland Security Presidential Directive - 8 (i.e. the "National Preparedness Goal") and the National Infrastructure Protection Plan (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.

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. • The NIMS Capability Assessment Support Tool (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 NIMS Integration Center 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. The NIMS Capability Assessment Support Tool (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 NIMS Integration Center (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 N

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 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.

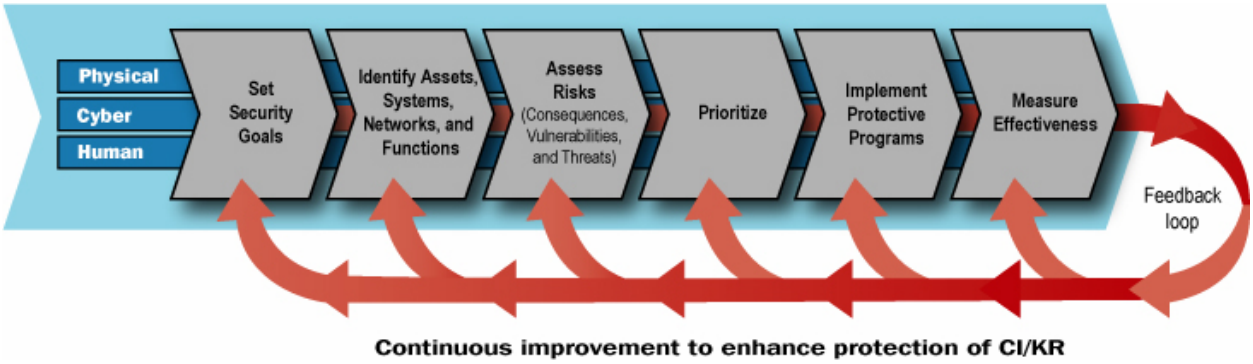
- **Identify assets, systems, networks, and functions:** Develop an inventory of the assets, systems, and networks, including those located outside the United States, that compose the Nation's infrastructure and the critical functionality therein; collect information pertinent to risk management that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



Continuous improvement to enhance protection of CI/KR

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 Sector-Specific Agencies (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 grant 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 O

PUBLIC SAFETY COMMUNICATIONS AND INTEROPERABILITY GUIDANCE

Public Safety Communications and Interoperability Guidance

A. Introduction

One of the major issues facing the Emergency Services Sector is the inability of emergency service workers, including traditional "first responders," to communicate with one another when the need arises. These emergency first responders have long been defined as the "first arriving organized responders with the capability and mission to contain, mitigate, and resolve the emergency at hand." Their effective and efficient emergency response requires coordination, communication, and sharing of vital information among numerous public safety agencies. As the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* observes, "Most systems supporting emergency response personnel, however, have been specifically developed and implemented with respect to the unique needs of each agency." Such specification without regard to the need for interoperability tends to complicate the ability of those agencies to effectively communicate with others in the future—a problem echoed by the public safety community in the National Task Force on Interoperability report: *Why Can't We Talk - Working Together To Bridge the Communications Gap to Save Lives.*

In line with the needs of public safety and the national strategy, Fiscal Year 2006 Appropriations make grant funding available to improve the effectiveness of public safety communications systems and to resolve interoperability shortfalls. By definition, communications interoperability refers to the ability of public safety agencies to talk across disciplines and jurisdictions via radio communications systems and to exchange voice and/or data with one another on demand, in real time, when needed, and as authorized. The Federal program offices recognize that many law enforcement, fire service, emergency medical service and other emergency response personnel currently lack effective and modern communication systems within their respective organizations. The programs support the need to improve those systems so long as the improvement planning includes a vision for improved interoperability with other agencies. Additionally, the programs require emergency response agencies developing systems to improve communications and interoperability to ensure that their solutions are compliant with the concepts, processes, and protocols set forth in the NIMS. In an effort to coordinate the way in which funding is allocated and to maximize the prospects for interoperable communications, some general grant criteria have been developed in concert with representatives of the public safety community. What follows is an outline of grant applicant eligibility, purposes for grant fund usage and guidelines for implementing a wireless communications system.

This appendix provides general criteria relating to public safety communications grants, suggested considerations based on the lifecycle of public safety communications projects and further criteria specific to block grants allocated to states, as well as additional guidelines, examples and resources for improving public safety communications and interoperability.

B. General Public Safety Communications Related Grant Criteria

1. Who should be involved with Public Safety Communications Interoperability

Federal funds that are allocated for improving public safety communications and interoperability should only be provided to public safety agencies or organizations at the regional, state, local, or tribal, level. This includes:

- Emergency Medical Services (EMS) agencies
- Fire Service agencies
- Law Enforcement agencies
- An organization representing the aforementioned agencies

2. Lifecycle of Public Safety Communications Projects

While applying for equipment grants, applications should be capable of addressing each of the following aspects within the lifecycle of public safety communications:

- *Planning* for public safety communication systems
- *Designing* public safety communication systems
- *Building* public safety communication systems
- *Developing* operational and technical policies and procedures
- *Upgrading/enhancing* public safety communication systems and equipment
- *Replacing* public safety communication systems and equipment
- *Maintaining* public safety communication systems and equipment
- *Training* public safety staff on procedures for interagency communications
- *Exercising* public safety procedures and systems
- *Using* public safety interoperability solutions regularly to ensure ongoing familiarity
- *Managing* public safety communications projects

C. Common Public Safety Communications Goals

Grants will be awarded to applicants that aim to achieve the following goals identified and supported by the public safety community and each grant-making agency.

- Applicants should provide a clear and measurable plan for communications interoperability between first responders of regional, state, local, and tribal public safety agencies or other partnering agencies or organizations from Federal, regional, state, local, and tribal jurisdictions, particularly in times of natural disaster and major criminal or terrorist acts. Measurable means the goals and objectives of the plan, wherever possible, are quantifiable, and the plan reflects how it contributes to achieving interoperable communications for the grant recipient and for the Nation.

- Applicants should demonstrate how funds would be used to upgrade or enhance "mission critical" networks with interoperable communications equipment for

everyday use to ensure the safety and well-being of first responders and the public they serve. The National Task Force on Interoperability defined mission critical as "Transmissions necessary for the preservation of life and property." The *Final Report of the Public Safety Wireless Advisory Committee* adds further clarification: "A mission critical communication is that which must be immediate, ubiquitous, reliable, and, in most cases, secure. Mission critical communications require the highest level of assurance that the message will immediately be transmitted and received regardless of the location of the operating units within the designed coverage area."

D. Common Criteria for All Grant Applicants

In order to receive funding, the applicant must be able to convey an understanding of the first responder needs and a clear path towards interoperability. Each grant application must explain how the proposed project would fit into an overall effort to increase interoperability. Even if the funding sought is only for a piece of an interoperability endeavor (i.e., training for staff, procurement of new equipment), an executive summary should be provided to illustrate the broader context of the agency/jurisdiction's interoperability plans. Such an explanation could include information on the governance structure overseeing the effort, a communications system plan, a deployment plan, an operations, maintenance and training plan, and a financial plan.

At a minimum, the applicant must:

- Define the vision, goals, and objectives of what the applicant is ultimately trying to accomplish and how the proposed project would fit into an overall effort to increase interoperability, including integration into regional and state plans/strategies;
- Describe the specific problems or needs that are to be addressed;
- Identify any potential partners and their roles and staffing requirements, and provide information on any existing agreements such as a Memorandum of Understanding (MOU) or Mutual Response Agreement (MRA);
- Propose a detailed budget and timeline; and,
- Include an operational plan that addresses how the effort will be funded now and in the future.

E. Standards

When procuring equipment for communication system development and expansion, a standards-based approach should be used to begin migration to multi-jurisdictional and multi-disciplinary interoperability. Specifically, all new voice systems should be compatible with the Project 25 (P25) suite of standards. This recommendation is intended for government-owned or -leased land mobile public safety radio equipment, and its purpose is to make sure that such equipment or systems are capable of interoperating with other public safety land mobile equipment or systems. It is not

intended to apply to commercial services that offer other types of interoperability solutions and does not exclude any application if it demonstrates that the system or equipment being proposed will lead to enhanced interoperability.

With input from the user community, these standards have been developed to allow for backward compatibility with existing digital and analog systems and to provide for interoperability in future systems. The Federal Communications Commission (FCC) has chosen the P25 suite of standards for voice and low-moderate speed data interoperability in the new nationwide 700 MHz frequency band, and the Integrated Wireless Network (IWN) of the U.S. Justice and Treasury Departments has chosen the P25 suite of standards for their new radio equipment. P25 has also been endorsed by the U.S. Department of Defense for Land Mobile Radio (LMR) systems.

However, the first priority of Federal funding for improving public safety communications is to provide basic, operable communications within a department with safety as the overriding consideration. Funding requests by agencies to replace or add radio equipment to an existing non-P25 system will be considered if there is an explanation as to how their radio selection will allow for improving interoperability or eventual migration to interoperable systems. This guidance does not preclude funding of non-P25 equipment when there are compelling reasons for using other solutions. Absent these compelling reasons, SAFECOM intends that P25 equipment will be preferred for digital systems to which the standard applies.

F. Governance

There needs to be consistent leadership and management to ensure that the planning, equipment procurement, training and funding are in place when developing a public safety communications improvement or interoperability project. A common governing structure should improve the policies, processes and procedures of any major project by enhancing communication, coordination and cooperation; establishing guidelines and principles; and, reducing any internal turf battles. This group should consist of Federal, state, local and tribal entities as well as representatives from all pertinent public safety disciplines. Frequently, when multiple agencies/jurisdictions are involved, this management is in the form of a governing body that makes decisions, solicits funding and oversees the implementation of an interoperability initiative.

G. Additional Criteria on the Lifecycle of Public Safety Communications Projects

Planning for, building, upgrading, enhancing, replacing, maintaining, training staff and managing projects for a public safety communications system are arduous tasks that require both short- and long-term strategies. Whether it is the development of a technical plan, training exercise or system upgrade, any effort that ultimately leads to improved interoperability must include participation from all of the relevant agencies, jurisdictions or other organizations that contribute to an effective emergency response.

This participation is frequently exhibited through a governing structure that improves the process of any major project by enhancing communication, coordination and cooperation; establishing guidelines and principles; and, reducing any internal turf battles. This group should consist of Federal, state, local and tribal entities, as well as representatives from all pertinent public safety disciplines.

Answers to the following questions will help provide the applicant with a fuller vision of how the proposed project or effort will ultimately improve interoperability. Sections addressing the building, upgrading, enhancing, replacing phases of the lifecycle have been grouped together as they address needs and recommendations specific to public safety communications equipment.

1. *Planning* for Public Safety Communication Systems

There are three types of planning for public safety communications: operational, technical and governance. Operational planning for public safety communications projects includes defining standard operating procedures, training/exercises and regular use for the equipment. Technical planning for public safety communications projects may include needs and requirements assessments, development of the system network architecture, propagation studies and similar technical proposals. Governance planning for public safety interoperability projects may include development of needs assessments, strategic plans and financial plans. Questions that an applicant for communication systems planning funds should address are listed below.

The following questions will provide the grant-making agencies with an understanding of the applicants planning efforts:

Has the applicant considered the communication needs and requirements of its public safety community?

- With whom does the agency/jurisdiction need to communicate?
- How does the agency/jurisdiction need to communicate?
- What information needs to be exchanged?
- When does the agency/jurisdiction need to communicate and exchange information (i.e., daily, weekly, infrequently)?
- Under what circumstances does the agency/jurisdiction need to communicate (i.e., frequently occurring emergencies, major crimes or incidents, large-scale disasters)?

Does the applicant plan to include nearby agencies/jurisdictions from other disciplines or other Federal, state, local, or tribal partners in its planning effort?

- Who are the stakeholders that need to be involved in the planning?
- Which decision makers should be involved in planning?
- What type of technical and field expertise will be needed to develop the plan?
- Will outside expertise be needed to develop this plan?

- What are the roles and responsibilities of all agencies that are involved? (Include a list of partnering agencies.)
- Are there any mutual response agreements in place?
- What type of governing structure exists to improve the processes involved in executing any planned project?

Does the potential plan take into account both short- and long-term goals?

- What should be done in the first phase (most critical)?
- How many phases will the plan require?
- How much time is needed to accomplish the plan?
- What are the technical solutions available to address the problem?
- What funding is available to address the problem?

2. *Building, Upgrading, Enhancing, Replacing, and Maintaining* Public Safety Communications Systems and Equipment

Public safety interoperable communication grants can be used to build, upgrade, enhance, or replace communications equipment. Communication systems and equipment are expensive, and before a procurement decision is made, there must be an assessment of the current communication system and future needs. Additionally, funds should be directed at the improvement of existing systems, where applicable, rather than at the development of completely new infrastructure using proprietary equipment.

The following questions provide guidance for fulfilling public safety communications goals:

Has the applicant already completed a plan that illustrates the agency/jurisdiction's commitment to the aforementioned public safety priorities?

- Please provide an executive summary that clearly illustrates how the proposed effort will lead to enhanced public safety communications interoperability.
- What type of multi-jurisdictional or multi-disciplinary agreements does the agency possess (i.e., MOUs, interstate compacts, mutual response agreements)?

Has the applicant considered public safety's operational needs of the communications equipment?

- In what type of topography/terrain does the agency operate?
- In what types of structures does the agency need to communicate (i.e., tunnels, high-rise buildings)?
- What methods of communication does the agency use (i.e., e-mail, paging, cellular calls, portable radio communications)?
- What is the process for dispatching calls?
- Is the communications center independently owned and operated by the agency? Does it serve several public safety agencies in the jurisdiction? Is it a multi-agency, multi-jurisdictional facility?

- Does the agency have the ability to patch across channels? If so, how many patches can be simultaneously set up? Is a dispatcher required to set up and break the patches down?
- What is the primary radio language used by the agency when communicating with other agencies or organizations (i.e., 'plain' English, code)?
- What types of equipment can immediately be deployed to provide short-term solutions for improved communications?

Has the applicant considered the system requirements to ensure interoperability with systems used by other disciplines or other levels of government?

- What type of equipment is currently used by the agency?
- Is there a regional, multi-jurisdictional, or statewide system in place that requires interoperability in order to communicate with other agencies? If so, how will the applicant interoperate/connect to that system?
- Is the equipment compatible with the P25 suite of standards?
- For data-related systems, is the applicant using XML standards?
- How scalable is the system? Can it be used locally between agencies and jurisdictions, statewide, and at a multi-state or national level?
- What internal and external security requirements exist in the architecture to secure information and maintain privacy levels for data as required by law?
- Is the infrastructure shared with any other agency or organization? Is it owned or leased?
- Does the agency use analog or digital radio systems or both?
- Is the system conventional or trunked?
- Which radio frequencies are used to communicate with other public safety agencies?
- How many channels does the agency have solely designated for communicating with other agencies?

Has the applicant considered a plan for backup communications capabilities in the event that the primary communications systems are significantly damaged or otherwise unable to function?

- Will equipment caches be in place?
- Are survey teams available for quick deployment to assess damages?
- Who will lead the effort?

3. *Training* Public Safety Staff on Issues Related to Emergency Response Communications

For equipment to be used properly and effectively in emergency situations, Emergency Service personnel must be trained through joint exercises that afford them the ability to practice standard operating procedures, become familiar with the equipment, and enhance their capacity and preparedness to respond to all types of emergencies. Eligible applicants should exhibit multi-disciplinary and multi-jurisdictional training in their overall public safety communications plan.

Do the applicant's training plans include exercises with other agencies/jurisdictions?

- Do the agency's training plans include participation from all levels and functions of emergency response (i.e., Federal, state, local, fire, law enforcement, emergency medical services)?
- How often will training take place?
- Who will conduct the training?
- Where will the training be held? Will it be onsite or at a specified training facility?
- What maintenance efforts will exist to keep personnel up to date with changes in procedure, equipment functions, or other relevant policies?
- How will lessons learned from training exercises be applied to operational procedures? Will there be post-exercise evaluations or analyses?

4. *Managing* Public Safety Communications Projects

There needs to be consistent leadership and management to ensure that the planning, equipment procurement, training, and funding are in place when developing a public safety communications improvement or interoperability project. Frequently, when multiple agencies/jurisdictions are involved, this management is in the form of a governing body that makes decisions, solicits funding and oversees the implementation of an interoperability initiative. Organizations that govern such projects must be comprised of the relevant law enforcement, fire and emergency agencies in order to qualify for grant awards.

Is the communications project consistent with similar efforts in the region?

- Does the applicant have agreements in place with other agencies/jurisdictions that illustrate the cooperative and interoperable approach to managing the communications improvement or interoperability project?

Does the project have the support of the relevant governing body (state or local authority)?

- What other funding sources has the applicant sought for the ongoing administrative costs of program management?

5. *Using* Public Safety Emergency Response Communications Solutions

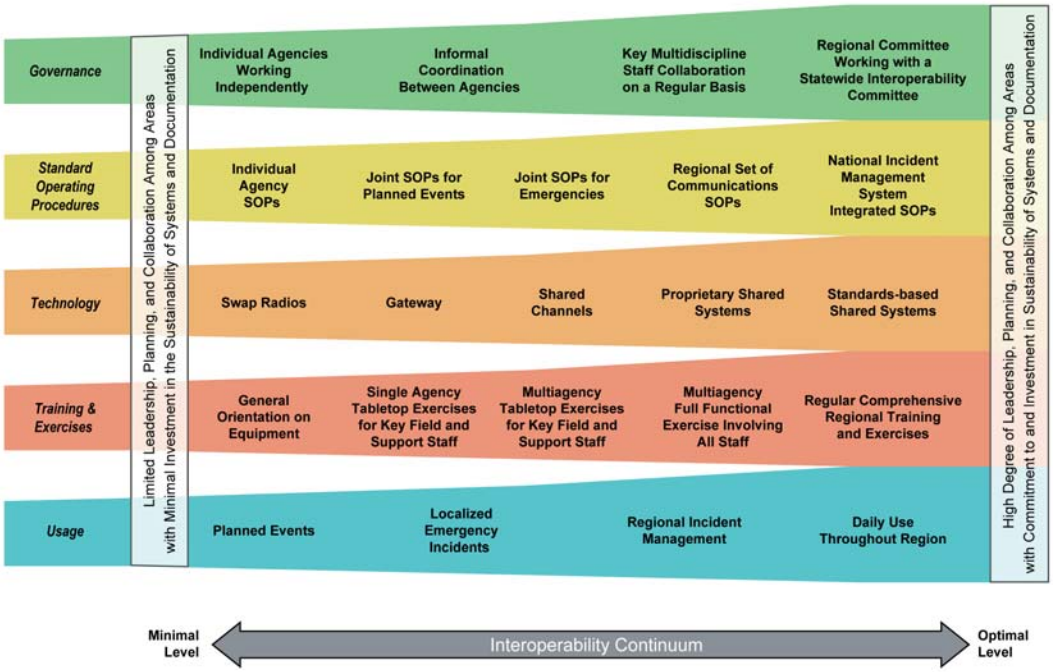
No matter the level of management, planning, technology, standard operating procedures and training that is adopted by an agency, interoperability solutions must be routinely used so that agency staff is familiar with the equipment and procedures. Emergency response personnel in high stress situations revert to using equipment and procedures that they are familiar with and are comfortable using. Thus, unless both operable and interoperable communications solutions are used as part of routine operations every day (as applicable), they will not be used during major incidents. Just as with an agency's general staff, its supervisors and command staff must likewise be familiar with the equipment and protocols required to use the various communications

solutions that are available to the agency if they are going to direct its activation; the best way to enforce this familiarity is through daily use of solutions.

H. Additional Guidelines for Implementing a Wireless Communications System

As an additional resource for any agency or region addressing communications and interoperability needs of its public safety community, the Interoperability Continuum is designed to help the public safety community and Federal, state, local and tribal policy makers address critical elements for success as they plan and implement interoperability solutions. The Continuum highlights that a number of different elements are essential to success, including frequency of use of the interoperable communications, governance, standard operating procedures, technology and training/exercises.

Movement along all elements of the Continuum is crucial as all elements are interdependent.



To drive progress on the Continuum and improve interoperability, public safety practitioners should:

- Gain leadership commitment from all disciplines (law enforcement, fire, EMS)
- Foster collaboration across disciplines through leadership support
- Interface with policy makers to gain leadership commitment and resource support
- Use interoperability solutions on a regular basis
- Ensure collaboration and coordination across all elements (frequency of use, governance, standard operating procedures, technology, training/exercises)

More detailed information on the Interoperability Continuum can be found on the SAFECOM Web site at http://www.safecomprogram.gov.

I. Generic Examples of Linking Disparate Public Safety Communications Systems

There are multiple approaches for linking disparate networks. Descriptions of common technologies are provided below.

1. Cross band/In-Band Repeater Gateways

Although there are more robust solutions available today, repeaters still provide improved interoperability for agencies needing to link disparate systems.

Cross band/in-band repeater gateways instantly retransmit signals input from one channel/system to another. These may be in the same or a different frequency band. Cross band repeaters range from simple devices supporting frequency transfers across two channels/bands (e.g., ultra high frequency [UHF] and very high frequency [VHF]) to more complex devices capable of bridging multiple frequency channels/systems/bands (e.g., UHF, VHF Low Band, VHF High Band, and 800 MHz). Within minutes after arriving on the scene of an incident, a portable gateway can be quickly programmed to support the frequencies of participating agency radios. Some of these solutions also allow access to disparate systems via the Public Switched Telephone Network (PSTN).

2. Network-to-Network Gateways

Numerous initiatives are already underway to implement short-term integration technologies that provide a reasonable level of interoperability among disparate networks.

Network-to-network gateways provide radio interoperability during missions requiring communications between diverse organizations using different systems and technologies across multiple frequency bands. Network-to-network gateways offer a standard way to link wireless infrastructures. These gateways are usually at fixed locations and often support the passing of more advanced features such as unit ID between participating systems. As with the prior solution, many of these gateways allow access to disparate systems via the PSTN, as well as to share data.
Minimum specifications have been developed for instances where gateway (either cross band/in-band or network-to-network) solutions are to be implemented. Where such interconnect devices are to be used, the following specifications should be followed:

- Operating Modes
  - The device must be able to retransmit the audio of radios that operate in different parts of the radio spectrum, use different modulation and access techniques, and use analog or digital encoding. The audio shall be distributed or switched throughout a shared audio distribution bus, where it

can be presented to and shared among all or a selected subset of radios interfaced to the device.

- Capacity
  - The device must support a minimum of four LMR in different operating modes. The ability to support cellular phones and connection to PSTN is desirable.
- Power Sources and Physical Features
  - The device must be capable of being powered either from vehicular power, battery power, or portable AC power sources.
  - The device must accommodate being rack mounted or standing alone in a portable enclosure. The device must be able to withstand shock and vibration typically encountered in field operations activity.
  - The device must include documented cable specifications for audio (speaker and microphone) and control (push-to-talk, or PTT) in order to interface with the basic audio and transmit controls for standard off-the-shelf LMR manufacturers' subscriber units that are typically employed by public safety.
  - The device must have input mechanisms or modules that can support balanced or unbalanced two- or four-wire circuits.
  - The device must have input mechanisms or modules that can transmit (TX) audio, receive (RX) audio, PTT, and Carrier Operated Relay/Carrier Operated Squelch (COR/COS) signaling. Ability for supporting Tone Remote Control (TRC) and Voice Operated Transmit (VOX) signaling is desirable. Some form of adjustable automatic gain control should be provided for each device interface.
- Control and Administration
  - The device must provide local control to establish two or more talk groups of the radios/phone interfaces that are provided.
  - The device must provide adjustable audio/PTT delay to the radio interfaces to allow the supported radios and associated infrastructure to reach full transmit power and to accommodate unknown repeater operating parameters such as hang times and squelch trails.
  - The device must be easily configurable with short set up times.

3. Console Interfaced Gateways

Similar to fixed network-to-network gateways, some consoles provide similar support either manually or electronically. Console interfaced gateways (i.e., "patches") route audio signals from one channel or system to other channels and/or systems through a dispatch console, either by dispatcher intervention or by a pre-wired configuration through the console electronics, thereby supporting direct connections between disparate systems.

4. Shared Networks

Many states and regions have significant investments in large-scale, shared networks, briefly described below. These networks offer a high degree of interoperability within

their geographic coverage areas and can be linked to other networks through network-to-network gateways. Some of these networks meet the P25 suite of standards.

Shared networks have common backbone infrastructures and interfaces. These are often single vendor solutions covering large geographic areas and/or commercial networks. The typical model calls for participating jurisdictions to purchase subscriber radios compatible with the network and to pay a monthly service fee.

APPENDIX P

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 interagency 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 TSGP 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.

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 Q

ACRONYMS AND ABBREVIATIONS

Acronyms and Abbreviations

A		
	AAR	After Action Reports
	ACH	Automated Clearing House
	AG	Automated Guideway
	AEL	Authorized Equipment List
	AFG	Assistance to Firefighters Grant
	ANSI	American National Standards Institute
	AOR	Authorized Organization Representative
	ASAP	Automated Standard Application for Payments
B		
	BSIR	Biannual Strategy Implementation Reports
	BZPP	Buffer Zone Protection Program
C		
	CAP	Corrective Action Plan
	CAPR	Categorical Assistance Progress Reports
	CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
	CC	Cable Car
	CCR	Central Contract Registry
	CCTV	Closed Circuit Television
	CEQ	Council on Environmental Quality
	CFDA	Catalog of Federal Domestic Assistance
	CFR	Code of Federal Regulations
	CI/KR	Critical Infrastructure/Key Resource
	CMC	Crisis Management Center
	CMIA	Cash Management Improvement Act
	COR/COS	Carrier Operated Relay/Carrier Operated Squelch
	CRWG	Comprehensive Review Working Group
	CPTED	Crime Prevention Through Environmental Design
	CSID	Centralized Scheduling and Information Desk
D		
	D&B	Dun and Bradstreet
	DHS	U.S. Department of Homeland Security
	DLA	Defense Logistics Agency
	DNDO	Domestic Nuclear Detection Office
	DOE	U.S. Department of Energy
	DOT	U.S. Department of Transportation
	DUNS	Data Universal Numbering System
E		
	EA	Environmental Assessment
	EIS	Environmental Impact Statement
	EMI	Emergency Management Institute
	EMS	Emergency Medical Service
	EOC	Emergency Operations Center
	EOP	Emergency Operations Plans

	ESF	Emergency Support Functions
F		
	FAR	Federal Acquisition Regulations
	FCC	Federal Communications Commission
	FICA	Federal Insurance Contributions Act
	FOIA	Freedom of Information Act
	FSR	Financial Status Report
	FTA	Federal Transit Administration
	FTE	Full-Time Employees
	FJ	Funding Justification
	FY	Fiscal Year
G		
	G&T	Office of Grants and Training
	GAN	Grant Adjustment Notice
	GMS	Grants Management System
	GPS	Global Positioning Systems
H		
	HDER	Homeland Defense Equipment Reuse
	HHS	U.S. Department of Health and Human Services
	HRSA	Health Resources and Services Administration
	HSEEP	Homeland Security Exercise and Evaluation Program
	HSGP	Homeland Security Grant Program
	HSIN	Homeland Security Information Network
	HSOC	Homeland Security Operations Center
	HSPD	Homeland Security Presidential Directive
	HSPTAP	Homeland Security Preparedness Technical Assistance Program
I		
	IAB	Interagency Board
	ICS	Incident command system
	ICTAP	Interoperable Communications Technical Assistance Program
	ID	Identity
	IED	Improvised Explosive Device
	IEDDA	International Explosive Detection Dog Association
	IP	Improvement Plan
	IPP	Infrastructure Protection Program
	ISAC	Information Sharing & Analysis Center
	IWN	Integrated Wireless Network
J		
	JIC	Joint Information Center
	JIS	Joint Information System
	JTTF	Joint Terrorism Task Force
L		
	LEP	Limited English Proficiency
	LLIS	Lessons Learned Information Sharing
	LMR	Land Mobile Radio
	LOCES	Letter of Credit Electronic Certification System
M		
	M&A	Management and Administrative

MARSEC	Maritime Security
MIPT	Memorial Institute for the Prevention of Terrorism
MO	Monorail
MOU	Memorandum of Understanding
MPIN	Marketing Partner Identification Number
MRA	Mutual Response Agreement
MT/HSAP	Mass Transit Homeland Security Assistance Program
MTSA	Maritime Transportation Security Act

N

NCJA	National Criminal Justice Association
NEPA	National Environmental Policy Act
NGO	Non-governmental Organization
NIC	NIMS Integration Center
NIJ	National Institute of Justice
NIMCAST	NIMS Capability Assessment Support Tool
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NPCA	National Police Canine Association
NPG	National Preparedness Guidance
NRP	National Response Plan
NSHS	National Strategy for Homeland Security
NSSE	National Security Special Events
NSTS	National Strategy for Transportation Security
NTD	National Transit Database

O

OC	Office of the Comptroller
OCC	Operations Control Center
OCMI	Officer in Charge of Marine Inspection
OGO	Office of Grant Operations
OIC	Office for Interoperability and Compatibility
OJP	Office of Justice Programs
OGC	Office of General Counsel
OMB	Office of Management and Budget

P

PAPRS	Phone Activated Paperless Request System
POC	Point of Contact
POETE	Planning, Organization, Equipment, Training, and Exercises
PORR	Program Observation and Recommendation Report
PPE	Personal Protective Equipment
PROTECT	Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism
PSGP	Port Security Grant Program
PSTN	Public Switched Telephone Network
PTT	Push-to-Talk

R

RAD/NUC	Radiological/Nuclear
RDT&E	Research, Development, Test and Evaluation
RKB	Responder Knowledge Base

	RTSWG	Regional Transit Security Work Group
	RTSS	Regional Transit Security Strategy
S		
	S&T	Science and Technology
	SAA	State Administrative Agency
	SEL	Standardized Equipment List
	SEPP	Security and Emergency Preparedness Plan
	SOP	Standard Operating Procedures
	SPOC	Single Point of Contact
	SSI	Sensitive Security Information
	SSA	Sector Specific Agency
	SSP	Sector-Specific Plan
T		
	TA	Technical Assistance
	TCL	Target Capabilities List
	TEW	Terrorism Early Warning
	TIA	Terrorism Incident Annex
	TISD	Transportation Infrastructure Security Division
	TPIN	Trading Partner Identification Number
	TRC	Tone Remote Control
	TSA	Transportation Security Administration
	TSGP	Transit Security Grant Program
	TSOC	Transportation Security Operations Center
	TSI	Transportation Security Incident
U		
	UASI	Urban Area Security Initiative
	UAWG	Urban Area Working Group
	USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
	USC	United States Code
	USPCA	United States Police Canine Association
	UTL	Universal Task List
V		
	VOX	Voice Operated Transmit
W		
	WMD	Weapons of Mass Destruction