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

FY 2006 Infrastructure Protection Program: *Trucking 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) Trucking Security Grant 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, $3 million is available for a package of related infrastructure protection grants. The FY 2006 Trucking Security Program makes up $5 million of the total infrastructure protection grant funds available.

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 to make our nation safer in the war against terror. Specifically, with respect to trucking security:

- The Transportation Security Administration has 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 Trucking Security Program (TSP) 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 trucking security grant.

---

[*] As this grant guidance went to print, the final Goal and the NIPP are being prepared for release.

II. The FY 2006 Trucking Security Program

> *The mission of the FY 2006 Trucking Security Program (TSP) is to sustain the Highway Watch® Program to enhance homeland security through increased vigilance and awareness on our Nation's highways.*

A. Program Overview

As a component of the Infrastructure Protection Program (IPP), the FY 2006 TSP seeks to assist all professionals and operating entities throughout the entire highway sector in obtaining the skills and abilities required to support the Goal and the associated National Priorities. Through its focus on awareness training, reporting of suspicious incidents and information analysis, the FY 2006 TSP directly addresses six of the seven National Priorities:

1) Expanded regional collaboration;
2) Implementing the National Incident Management System (NIMS) and the National Response Plan (NRP);
3) Implementing the NIPP;
4) Strengthening information sharing and collaboration capabilities;
5) Strengthening interoperable communications; and,
6) Chemical, biological, radiological, nuclear and explosive (CBRNE) detection and response capabilities.

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

The TSP was originally developed in the trucking industry with an emphasis on safety. It has undergone a dramatic expansion with the grant funds provided by DHS in the three years from FY 2003 to FY 2005, and its benefits and resources are now available to all professionals and operating entities throughout the highway sector, including private companies, public entities and governmental operations.

The program provides resources and services, free of charge, to commercial bus and motorcoach operators, and school bus owners and operators; governmental entities; the companies and entities that build and maintain the highways; highway cargo facility operators and brokers; support operations such as visitors centers, truck and bus support, and maintenance operations; commercial driver training schools and facilities; operators of private truck fleets; public safety personnel, including law enforcement, who respond to emergencies on the highways; and any and all additional entities or stakeholder segments identified by the American Trucking Associations (ATA) or Transportation Security Administration (TSA). By continuing to expand the scope of the existing Highway Watch® Program to encompass additional motor carriers and drivers in every state, territory, and Federal district in the country, all segments of the commercial motor carrier and transportation community can contribute to the security of the Nation. A response center has been established to communicate with active

program participants and to link with the transportation-based Information Sharing and Analysis Centers (ISAC).

The TSP is a cooperative agreement program. In this grant, the Secretary of Homeland Security looks to TSA to provide subject matter expertise that will inform decisions about the activities conducted by the recipient under the TSP. DHS G&T will provide grant management services to support the award. The nature of the Federal involvement in the execution of this program may range from joint conduct of a project to prior approval of a new project or the next phase of an approved project. Examples of substantial involvement include the following:

> Collaboration, participation, and/or intervention in any activity covered by the cooperative agreement;

> Approval from TSA, through DHS G&T, prior to the selection of a new project or commencement of the next phase of an approved project;

> Authority for TSA, through DHS G&T, to halt an activity if detailed performance specifications are not met;

> Authority for TSA, through DHS G&T, to direct or redirect the scope of work of a project based on new circumstances; and,

> Authority for TSA, through DHS G&T, to create a working group of key Federal and private sector stakeholders to provide guidance and coordination for Highway Watch® activities.

B. Solicitation Overview

The FY 2006 TSP is the fourth round of grants and builds upon the previous three rounds. The intent of the TSP is to maintain a sustainable national Highway Watch® program to enhance homeland security through increased vigilance and awareness on our Nation's highways.

The FY 2006 TSP will provide financial assistance to ATA to continue to facilitate training and reporting of suspicious activities on our Nation's highways. The program is administered by TSA in coordination with DHS G&T.

C. Project Selection

The FY 2006 TSP is a noncompetitive, discretionary assistance program. *Eligibility for funding is limited to the Highway Watch® program, an initiative of ATA. Project selection will be limited to continuing and expanding the four project priorities identified in Section IV: Program and Application Requirements.*

III. Eligible Applicant and Funding Availability

A. Eligible Applicant

The FY 2006 DHS Appropriations Act provides discretionary funds for a financial assistance program to support and expand the existing TSP. Eligibility for funding under this program is limited to the ATA.

B. Funding Availability

The FY 2006 TSP will provide **$4,801,500**. Funding will be provided directly ATA.

IV. Program and Application Requirements

A. General Program Requirements

ATA will be responsible for administration of the FY 2006 TSP award. In administering the program, the ATA must comply with the following requirements:

1. **Management and Administrative Costs.** Any management and administration (M&A) costs associated with individual projects submitted for consideration of funding under the FY 2006 TSP must be included in the budget for that project. M&A costs associated with managing the overall TSP award itself must be accounted for separately.

B. Specific Program Requirements

The FY 2006 TSP will continue to encompass additional motor carriers, drivers and transportation professionals in every state, territory, and Federal district in the country. *The following four categories must each be addressed in a separate project plan:*

1. **Participant Identification and Recruitment:**

   ➢ <u>Motor Carriers</u> – Develop methodologies to identify and recruit new motor carriers (e.g., truck, bus, truck driving schools, school transportation) that will actively participate in and support Highway Watch® training;

   ➢ <u>Individual Drivers</u> – Develop methodologies to identify and recruit active current drivers to include independent, unaffiliated drivers, passenger carriers, and other vehicle fleets to expand the program;

   ➢ <u>Responder/Law Enforcement</u> – Develop methodologies to identify and recruit first responder/enforcement entities that will actively support Highway Watch® goals regarding driver training.

2. **Training:**

   ➢ Develop an evaluation methodology to ensure that the Highway Watch® training program is addressing homeland security and safety issues in conjunction with the Goal.

   ➢ Develop and implement a training component specific to state, local and municipal law enforcement entities to familiarize these forces with the domain awareness and incident/suspicious activity reporting training afforded to Highway Watch students and with the identification devices used to distinguish Highway Watch-trained personnel from those who have not been trained.

3. Communications:

➢ <u>Highway Watch Call Center</u> – Assist in maintaining a full-service (24/7) communications/call center staffed with well-trained responders who will provide nationwide first responder and law enforcement contact numbers and electronic linkage to registered participants. The center must be capable of re-directing calls to law enforcement and first responders for immediate action or to the Highway ISAC for investigation as terrorist threats. The call center may be utilized during an incident of national significance.

4. Information Analysis and Distribution:

➢ The applicant will provide management consulting services and oversight in cooperation with TSA leadership to maintain the Highway ISAC, located at TSA's Transportation Security Operations Center (TSOC) in Herndon, VA and dedicated exclusively to highway and highway-transport related security needs and issues. The applicant will provide recommendations, implementation strategies, and a completed plan for continued Highway ISAC operations to include other transportation stakeholders. Responsibilities may include identifying the appropriate role of a highway-specific ISAC or implementation strategies that address incidents of critical national significance.

C. Ineligible Costs

Federal employees are prohibited from serving in any capacity (paid or unpaid) on any proposal submitted under this program. Federal employees may not receive funds under these awards.

The following costs are unallowable under the FY 2006 TSP:

➢ Maintenance Costs;
➢ Monthly service charges or recurring costs;
➢ Construction and renovation costs.

D. Cost Sharing or Matching

There is no match requirement for this program; however, G&T encourages cost sharing. Any matching funds shall be obligated during the project period. For further information on allowable sources and types of funds, timing of match contributions and records for match, please refer to the Office of Grant Operations (OGO) *Financial Management Guide*, available at http://www.dhs.gov/dhspublic/display?theme=18.

E. 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. **Applicants must apply for FY 2006 TSP funding at http://www.grants.gov. Complete applications must be received by G&T no later than 11:59 pm EST on August 4, 2006.**

2. On-Line Application

The on-line application must be completed and submitted by an authorized representative of the applicant organization 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;
➢ JP Form 4000/3, Assurances;
➢ JP form 4061/6, Certifications; and,
➢ Non-Supplanting Certification.

The program title listed in the Catalog of Federal Domestic Assistance (CFDA) is *"Truck Security Program".* The CFDA number is **97.059**. When completing the on-line application the applicant should identify its submission as a new, non-construction application. The project period will be for a period not to exceed **30 months**.

Appendix K provides applicants with a set of Quick-Start Instructions for registering in Grants.gov in order to submit an application.

Appendix M provides a checklist of all items that must be included for your application to be considered complete. The applicant should refer to this checklist to ensure that all required application items are contained within the application before submitting the application in Grants.gov.

3. Program Information

The eligible applicant must submit one application for funding for all four individual project area categories. The application must include information on program contacts, an individual project plan for each of the project areas, and a detailed budget for each of the project areas. In addition, if the applicant intends to use funds for M&A costs associated with managing the overall TSP award itself, a separate budget must be submitted detailing these costs.

The applicant should use the following file name conventions for files attached in Grants.gov:

Name of Applicant_ Document Type
Example #1: ATA_Program Contacts
Example #2: ATA_Project Plan_Project1
Example #3: ATA_Project Budget_Project1
Example #4: ATA_Program Budget_M&A Costs

➢ **Program Contacts.** The applicant must identify specific point(s) of contact (POC) to work with DHS on the implementation of the FY 2006 TSP.

> *Appendix B provides a sample format for the Program Contacts.*

➢ **Individual Project Plans.** The application must clearly demonstrate an ability to provide deliverables consistent with the purpose of the program and with the guidance provided by DHS. As such, the application must include the following items in its project plan:

   o Identification of Project Category (e.g., participant identification and recruitment, training, communications, or information analysis and distribution);
   o Project Narrative providing:
      ▪ A succinct statement summarizing the project;
      ▪ Management capabilities, including a description of technical plans for the project and a biographical summary of key personnel,
      ▪ Challenges and impediments to completing the project along with the proposed solutions;
      ▪ Major new initiatives, including a chart showing milestones and target dates for project completion.
   o Project Timeline/Milestones.

The project period will be for a period not to exceed **30 months**. The project plan must not exceed five single-spaced pages and the type size shall not be smaller than 12 pitch/10 point type; page margins shall be no less than one inch from top and bottom, and left and right. Enter the title of the project priority on the top of each page of the attachment and number the pages. *The application must include an Individual Project Plan for each proposed project.*

> *Appendix C provides a sample format for the Individual Project Plans.*

➢ **Detailed Budgets.** The applicant must also provide a detailed budget for use of the funds requested. The budget must be complete, reasonable, and cost-effective in relation to the proposed project. The budget should describe the costs for each project component and provide the basis of computation of all project-related costs including any appropriate narrative. The budget should also

demonstrate any matching funds that will be offered. However, providing matching funds is *not* a program requirement.

The application must include a separate budget for each proposed project. If the applicant intends to use funds for M&A costs associated with managing the overall TSP award itself, a separate budget must be submitted detailing these costs.

Appendix A provides additional information on authorized program expenditures.

Appendix D provides a copy of the required budget worksheet.

4. **Universal Identifier**

   The applicant must provide a Dun and Bradstreet (D&B) Data Universal Numbering System (DUNS) number with the application. A final application will not be considered complete until the applicant provides a valid DUNS. 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.

   The applicant can receive a DUNS number at <u>no cost</u> by calling the dedicated toll-free DUNS Number request line at 1-800-333-0505.

5. **Freedom of Information Act (FOIA)**

   DHS recognizes that much of the information submitted in the course of applying for funding under this program, or provided in the course of its grant management activities, may be considered law enforcement sensitive or otherwise important to national security interests. This may include threat, risk, and needs assessment information, and discussions of demographics, transportation, public works, and industrial and public health infrastructures. While this information under Federal control is subject to requests made pursuant to the Freedom of Information Act (FOIA), 5. U.S.C. §552, all determinations concerning the release of information of this nature are made on a case-by-case basis by the DHS FOIA Office, and may likely fall within one or more of the available exemptions under the Act. The applicant is encouraged to consult its own state and local laws and regulations regarding the release of information, which should be considered when reporting sensitive matters in the grant application, needs assessment and strategic planning process. The applicant may also consult G&T regarding concerns or questions about the release of information under state and local laws. The Grantee 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. Use of Federal homeland security dollars for geospatial activities requires pre-approval and a demonstrated capability for robust interoperability with DHS and other relevant systems. G&T will coordinate review of requests for use of Federal homeland security funding for other geospatial projects with relevant entities.

7. Compliance with Federal Civil Rights Laws and Regulations

The Grantee is required to comply with Federal civil rights laws and regulations. Specifically, the grantee is required to provide assurances as a condition for receipt of Federal from DHS that its programs and activities comply with the following:

➢ *Title VI of the Civil Rights Act of 1964, as amended, 42. U.S.C. 2000 et. seq.* – no person on the grounds of race, color or national origin will be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination in any program or activity receiving Federal financial assistance;
➢ *Section 504 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. 794* – no qualified individual with a disability in the United States, shall, by reason of his or her disability, be excluded from the participation in, be denied the benefits of, or otherwise be subjected to discrimination in any program or activity receiving Federal financial assistance;
➢ *Title IX of the Education Amendments of 1972, as amended, 20 U.S.C. 1681 et. seq.* –discrimination on the basis of sex is eliminated in any education program or activity receiving Federal financial assistance;
➢ *The Age Discrimination Act of 1975, as amended, 20 U.S.C. 6101 et. seq.* – no person in the United States shall be, on the basis of age, excluded from participation in, denied the benefits of or subjected to discrimination under any program or activity receiving Federal financial assistance.

The grantee must comply with all regulations, guidelines, and standards adopted under the above statutes. The grantee is also required to submit information, as required, to the DHS Office for Civil Rights and Civil Liberties concerning its compliance with these laws and their implementing regulations.

8. **Financial Requirements**

   ➢ **Non-Supplanting Certification:** This certification affirms that these grant funds will be used to supplement existing funds, and will not replace (i.e., 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.

   ➢ **Match Requirement:** There is no match requirement for the FY 2006 TSP.

   ➢ **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 Grants.gov.***

   > *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 regulations 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 and cooperative agreements;

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

9. **Services to Limited English Proficient (LEP) Persons**

Recipients of DHS financial assistance are required to comply with several Federal civil rights laws, including Title VI of the Civil Rights Act of 1964, as amended. These laws prohibit discrimination on the basis of race, color, religion, 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. The grantee is encouraged to consider the need for language services for LEP persons served or encountered both in developing their proposals and budgets and in conducting their programs and activities. Reasonable costs associated with providing meaningful access for LEP individuals are considered allowable program costs. For additional information, 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.

V. Assistance Resources and Support

A. Drawdown and Expenditure of Funds

G&T's Office of Grant Operations (OGO) will provide fiscal support for 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 1-866-9ASK-OGO (1-866-927-5646) 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 subgrant 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 draw down and expend grant funds through the Automated Standard Application for Payments (ASAP), Phone Activated Paperless Request 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. The Grantee 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 both 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.

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 Grants Operations (OGO) will provide fiscal support and oversight of the
grant programs included in this solicitation. All grant and subgrant 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**.*

VI. Reporting, Monitoring and Closeout Requirements

A. Reporting Requirements

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, the 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. A copy of this form will be included in the initial award package. ***Future awards and fund drawdowns will be withheld if these reports are delinquent.***

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

The grantee is 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 Management Guide*. All previous awards are still governed by the OJP Financial Guide, available at http://www.ojp.usdoj.gov/FinGuide. OGO can be contacted by phone at 1-866-9ASKOGO or by email at ask-OGO@dhs.gov.

Required Submission: SF-269 (quarterly)

2. Categorical Assistance Progress Reports - OJP Form 4587/1

Following an award, the awardees will be responsible for providing updated obligation and expenditure information on a regular basis. The CAPR is 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 <u>January 30</u> with a reporting period of July 1 though December 31). Future awards and fund drawdowns may be withheld if these reports are delinquent. The final CAPR is due 90 days after the end date of the award period.

Block #12 of the CAPR should be used to note progress against the proposed project. The grantor agency shall provide sufficient information to monitor program implementation and goal achievement.

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

At a minimum, reports should contain the following data:

Output Indicators

➢ Total number of people trained in certified highway security domain awareness;
➢ Motor carriers/drivers identified/recruited/trained in the Highway Watch® Program;
➢ Calls received by the Highway Watch® Call Center;
➢ Calls received by the Highway ISAC; and,
➢ Training evaluation forms/results.

Outcome Indicators

➢ Number and percentage of annual training goals met.

The award recipient must include data pertinent to this measure within its CAPR submissions to G&T.

> **Required Submission**: CAPR (semiannually)

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 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 Government Accountability Office, *Government Auditing Standards*, located at http://www.gao.gov/govaud/ybk01.htm, and *OMB Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations*, located at http://www.whitehouse.gov/omb/circulars/index.html. Audit reports are currently due to the Federal Audit Clearinghouse no later than nine months after the end of the recipient's fiscal year. In addition, the Secretary of Homeland Security and the Comptroller General of the United States shall have access to any books, documents, and records of recipients of FY 2006 TSP 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.

For-profit organizations that expend $500,000 or more of Federal funds during their fiscal year shall have financial and compliance audits conducted by qualified individuals who are organizationally, personally, and externally independent from those who authorize the expenditure of Federal funds. This audit must be performed in accordance with Government Auditing Standards, 1994 Revision. The purpose of this audit is to ascertain the effectiveness of the financial management systems and internal procedures that have been established to meet the terms and conditions of the award. Usually, these audits shall be conducted annually, but not less frequently than every two years. The dollar threshold for audit reports established in OMB Circular A-133, as amended, applies.

B. Monitoring

Grant recipients will be monitored periodically by G&T program staff and OGO staff, 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. 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 subawards, 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.

C. Grant Closeout Process

Within 90 days after the end of the grant period, the grantee will submit a final SF-269a and a final CAPR detailing all accomplishments throughout the project. After both of these reports have been reviewed and approved by G&T, a Grant Adjustment Notice (GAN) will be completed to closeout 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 SF-269a.

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

APPENDIX A

AUTHORIZED PROGRAM EXPENDITURES GUIDANCE

Authorized Program Expenditures Guidance

This appendix serves as a guide for program expenditure activities. Within the four project areas (Participant Identification and Recruitment, Training, Communications, and Information Analysis and Distribution), funding may be used in the following categories:

1. Planning;
2. Training; and,
3. Management and Administration.

The applicant is encouraged to contact its G&T Program Manager regarding any questions about allowable and unallowable program expenditures.

A. Allowable Planning Costs

FY 2006 TSP funds may be used for the following types of planning activities:

➢ Public Education/Outreach;

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

➢ Development and enhancement of plans and protocols;

➢ Hiring of full- or part-time staff or contractors/consultants to assist with planning activities (not for the purpose of hiring personnel);

➢ Conferences to facilitate planning activities;

➢ Materials required to conduct planning activities;

➢ Travel/per diem related to planning activities; and,

➢ Other project areas with prior approval from TSA, through G&T.

B. Allowable Training Costs

FY 2006 TSP 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 applicant 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 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 sponsored 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 (e.g., 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-sponsored 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.

C. Allowable Management and Administrative (M&A) Costs

FY 2006 TSP funds may be used for the following M&A costs in the following manner:

➢ Hiring of full-time or part-time staff or contractors/consultants to assist with the management of the FY 2006 TSP;

➢ Hiring of full-time or part-time staff or contractors/consultants and expenses related to meet compliance with reporting/data collection requirements, including data calls;

➢ Meeting-related expenses (For a complete list of allowable meeting-related expenses, please review the OGO *Financial Management Guide*, available 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 ***dedicated solely to the use of TSP project activities***.

APPENDIX B

PROGRAM CONTACTS GUIDANCE

Program Contacts Guidance

The Program Contacts attachment must not exceed one page. The format below is strongly suggested for this file attachment. Please provide the following information for all projects proposed:

- ➢ Project title;
- ➢ Point of contact's (POC) name and title;
- ➢ POC's full mailing address;
- ➢ POC's telephone number;
- ➢ POC's fax number; and,
- ➢ POC's email address.

Please also include the corresponding information for your organization's authorizing official—i.e., the individual authorized to sign a cooperative agreement award—at the end of the Program Contacts file.

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

REMINDER: Please use the following file naming convention for this file attachment:

Name of Applicant_ Document Type
Example #1: ATA_Program Contacts

<u>APPENDIX C</u>

INDIVIDUAL PROJECT PLAN GUIDANCE

Project Plan Guidance

The applicant must submit an individual project plan for each project category within one application. Each Project Plan must not exceed five pages. The following format is strongly suggested for preparing each project plan file attachment:

Project Category

- ➢ Specify the category of focus for the project:
  - o Participant identification and recruitment;
  - o Training;
  - o Communications; and,
  - o Information analysis and distribution.

Project Narrative

- ➢ Provide a succinct statement summarizing the project;
- ➢ Complete the following statements: "This project will…" and "This project improves security by…";
- ➢ Describe any challenges and impediments to completing the project;
- ➢ Identify the proposed solutions;
- ➢ Describe the applicant's management capabilities;
- ➢ Include a description of technical plans for the project;
- ➢ Include a biographical summary of key personnel (at a minimum, this information should be provided for the POC identified in the Program Contacts file for the individual project);
- ➢ Describe any major new initiatives; and,
- ➢ Include a chart showing milestones and target dates for project completion.

Project Timelines/Milestones

- ➢ Outline the major project tasks and milestones from time of award until project completion:
  - o The project period may not exceed 30 months.
- ➢ For each task, provide:
  - o Short description of the task;
  - o Start date;
  - o Duration;
  - o Individual or organization responsible for the task; and,
  - o Description of how funds will be used to complete the task.

> *Important Note:* *The Individual Project Plan must demonstrate the organization's ability to continue and expand activities that address the four project priorities identified by G&T in Section IV.B. Ensure that the Project Plan is consistent with all applicable requirements outlined in this application kit.*

> *Important Note: This information may be provided using one of the attachment fields within Grants.gov.*

> **REMINDER:** The applicant must use the naming convention below when uploading the program narrative, individual project plans and budgets.
>
> Name of Applicant_ Document Type_ Project Number
> Example #2: ATA_Project Plan_Project1

APPENDIX D

BUDGET DETAIL WORKSHEET TEMPLATE

Budget Detail Worksheet Template

OMB Approval No. 1121-0188
Expires 5-98 (Rev. 12/97)

REMINDER: The applicant must provide a detailed budget for each proposed project. The applicant must use the naming convention below when uploading the project budget file(s). A separate budget detail worksheet should be provided for M&A costs as well as for each individual project.

Name of Applicant_ Document Type_ Project Number
Example #3: ATA_Project Budget_Project1; or
Example #4 : ATA_Budget_M&Acosts.

Budget Narrative: Provide a narrative budget justification for each of the budget items identified.

Purpose: The Budget Detail Worksheet may be used as a guide to assist you in the preparation of the budget and budget narrative. You may submit the budget and budget narrative using this form or in the format of your choice (plain sheets, your own form, or a variation of this form).   However, all required information (including the budget narrative) must be provided. Any category of expense not applicable to your budget may be deleted.

A. Personnel - List each position by title and name of employee, if available. Show the annual salary rate and the percentage of time to be devoted to the project. Compensation paid for employees engaged in grant activities must be consistent with that paid for similar work within the applicant organization.

Name/Position	**Computation**	**Cost**

TOTAL _____

B. Fringe Benefits - Fringe benefits should be based on actual known costs or an established formula. Fringe benefits are for the personnel listed in budget category (A) and only for the percentage of time devoted to the project. Fringe benefits on overtime hours are limited to FICA, Workman's Compensation, and Unemployment Compensation.

Name/Position	**Computation**	**Cost**

TOTAL _____
Total Personnel & Fringe Benefits _____

C. Travel - Itemize travel expenses of project personnel by purpose (e.g., staff to training, field interviews, advisory group meeting, etc.). Show the basis of computation (e.g., six people to 3-day training at $X airfare, $X lodging, $X subsistence). In training projects, travel and meals for trainees should be listed separately. Show the number of trainees and unit costs involved. Identify the location of travel, if known. Indicate source of Travel Policies applied, Applicant or Federal Travel Regulations.

Purpose of Travel	Location	Item	Computation	Cost

TOTAL _____

D. Equipment - List non-expendable items that are to be purchased. Non-expendable equipment is tangible property having a useful life of more than two years. (Note: Organization's own capitalization policy and threshold amount for classification of equipment may be used). Expendable items should be included either in the "Supplies" category or in the "Other" category. The applicant should analyze the cost benefits of purchasing versus leasing equipment, especially high cost items and those subject to rapid technical advances. Rented or leased equipment costs should be listed in the "Contractual" category. Explain how the equipment is necessary for the success of the project. Attach a narrative describing the procurement method to be used.

Item	Computation	Cost

TOTAL _____

E. Supplies - List items by type (office supplies, postage, training materials, copying paper, and other expendable items such as books, hand held tape recorders) and show the basis for computation. (Note: Organization's own capitalization policy and threshold amount for classification of supplies may be used). Generally, supplies include any materials that are expendable or consumed during the course of the project.

Supply Items	Computation	Cost

TOTAL _____

F. Consultants/Contracts - Indicate whether applicant's formal, written Procurement Policy or the Federal Acquisition Regulations are followed.

Consultant Fees: For each consultant enter the name, if known, service to be provided, hourly or daily fee (8-hour day), and estimated time on the project.

Name of Consultant	**Service Provided**	**Computation**	**Cost**

Subtotal _____

Consultant Expenses: List all expenses to be paid from the grant to the individual consultant in addition to their fees (i.e., travel, meals, lodging, etc.)

Item	**Location**	**Computation**	**Cost**

Subtotal _____

Contracts: Provide a description of the product or services to be procured by contract and an estimate of the cost. The applicant is encouraged to promote free and open competition in awarding contracts. A separate justification must be provided for sole source contracts in excess of $100,000.

Item	**Cost**

Subtotal _____
TOTAL _____

G. Other Costs - List items (e.g., rent, reproduction, telephone, janitorial or security services, and investigative or confidential funds) by major type and the basis of the computation. For example, provide the square footage and the cost per square foot for rent, and provide a monthly rental cost and how many months to rent.

Description   **Computation**   **Cost**

TOTAL _____

H. Indirect Costs - Indirect costs are allowed only if the applicant has a Federally approved indirect cost rate. A copy of the rate approval, (a fully executed, negotiated agreement), must be attached. If the applicant does not have an approved rate, one can be requested by contacting the applicant's cognizant Federal agency, which will review all documentation and approve a rate for the applicant organization, or if the applicant's accounting system permits, costs may be allocated in the direct costs categories.

Description   **Computation**   **Cost**

TOTAL _____

Budget Summary - When you have completed the budget worksheet, transfer the totals for each category to the spaces below. Compute the total direct costs and the total project costs. Indicate the amount of Federal funds requested and the amount of non-Federal funds that will support the project.

<u>Budget Category</u>	<u>Fed. Amount</u>	<u>Non-Fed. Amount</u>
A. Personnel	_____	_____
B. Fringe Benefits	_____	_____
C. Travel	_____	_____
D. Equipment	_____	_____
E. Supplies	_____	_____
F. Consultants/Contracts	_____	_____
G. Other	_____	_____
Total Direct Costs	_____	_____
H. Indirect Costs	_____	_____
* TOTAL PROJECT COSTS	_____	_____

Federal Request: _____

Non-Federal Amount: _____

> *Important Note: This information may be provided using one of the attachment fields within Grants.gov.*

> *Important Note: Cost-sharing is not a program requirement under the FY 2006 TSP. However, if matching funds are offered as part of the project, applicants are advised that an award recipient is responsible for meeting the matching funds reflected in an approved grant budget.*

<u>APPENDIX E</u>

ADDITIONAL GUIDANCE ON THE NATIONAL PREPAREDNESS AND THE NATIONAL PRIORITIES

A. The National Preparedness Goal[1]

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.[2] 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.

> *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.*

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.

---

[1] As this grant guidance went to print, the final Goal document was also being prepared for release.
[2] 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 F 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.[3] 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.[4] 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.[5]

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

---

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

needs. As indicated by the situation, response activities include: applying intelligence and other information to lessen the effects or consequences of an incident; increasing security and law enforcement operations; continuing investigations into the nature and source of the threat; continuing ongoing public health and agricultural surveillance and testing processes; providing immunizations; enforcing isolation or quarantine; and allowing appropriate citizen response.[6] 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.[7]

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.

---

[6] NIMS, March 2004.
[7] NIMS, March 2004.

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

B. The National Priorities

The National Priorities in the Goal help guide the Nation's preparedness efforts to meet its most urgent needs. The priorities fall into two categories: (A) Overarching priorities that contribute to the development of multiple capabilities, and (B) Capability-specific priorities that establish selected capabilities for which the Nation has the greatest need.[8] 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.

---

[8] 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.

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

B.1. <u>Expanded Regional Collaboration</u>

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. <u>Implement the NIMS and NRP</u>

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.

> *<u>Note</u>: 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 G 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 Port 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 H 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. <u>Strengthen Information Sharing and Collaboration Capabilities</u>

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. <u>Strengthen Interoperable Communications Capabilities</u>

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 I 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 J provides additional information on CBRNE threats and information on DNDO.

APPENDIX F

# 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
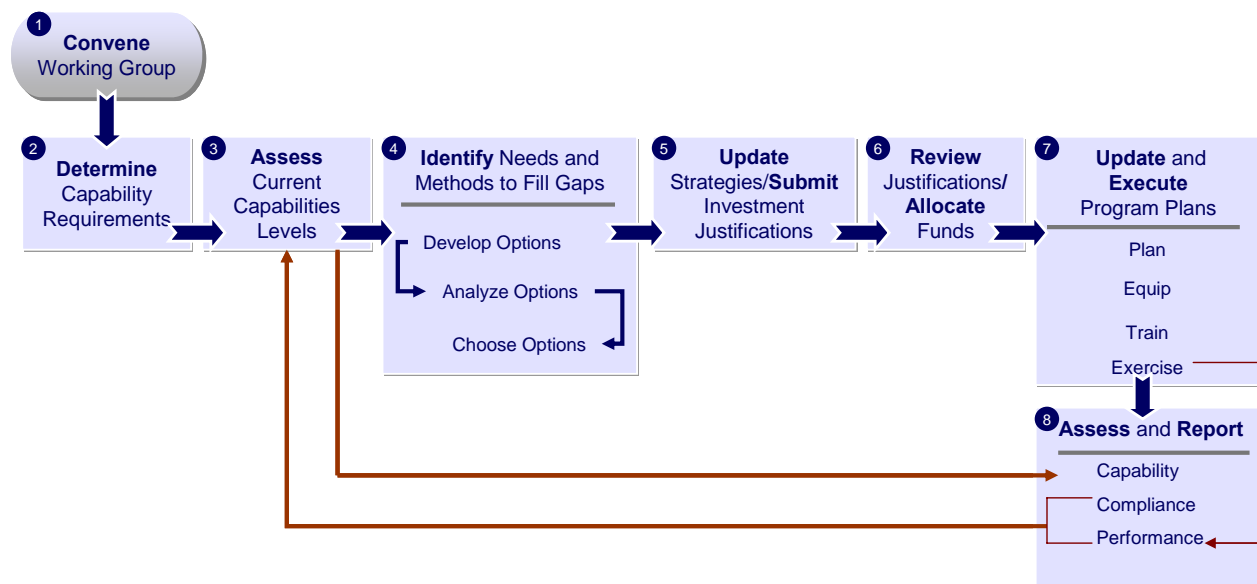
Step 1: Convene a Working Group

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.

Step 5: Update Strategies and Submit Investment Justifications

Once options are chosen, entities can update their preparedness strategies and prepare and submit annual investment 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. Investment justifications should identify prioritized resource needs to close capability gaps.

Step 6: Review Justifications and Allocate Funds

The review of investment justifications and allocation of funds occurs at all levels of government. At each level, relevant decision makers will lead a comparison of investment 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 G

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[9] 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[10] 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:

---

[9] 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)

[10] 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**
<u>Multi-agency Coordination System:</u> 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.
<u>Public Information System:</u> 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[11] and local[12] 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

---

[11] 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)

[12] 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		
<u>Incident Command System (ICS):</u> 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).

<u>APPENDIX H</u>

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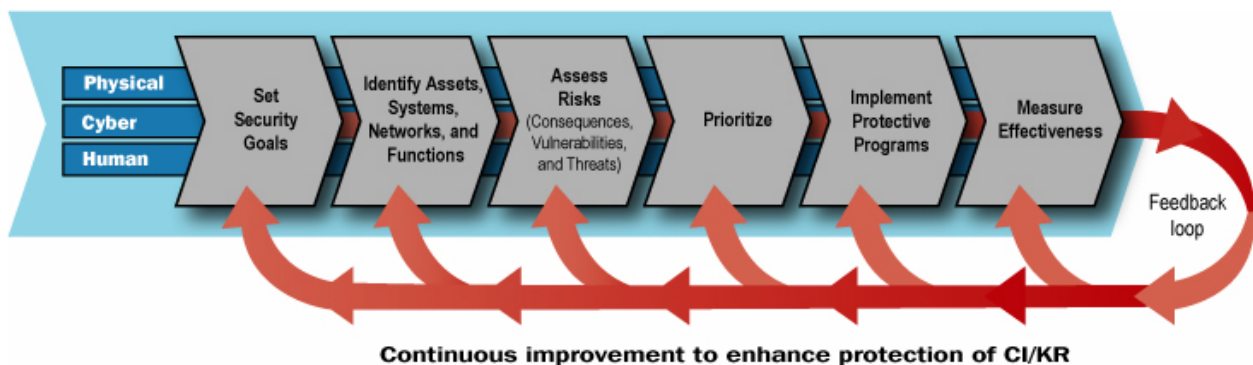
The NIPP provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort that brings together government at all levels, the private sector and international organizations and allies. In

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.

<u>APPENDIX I</u>

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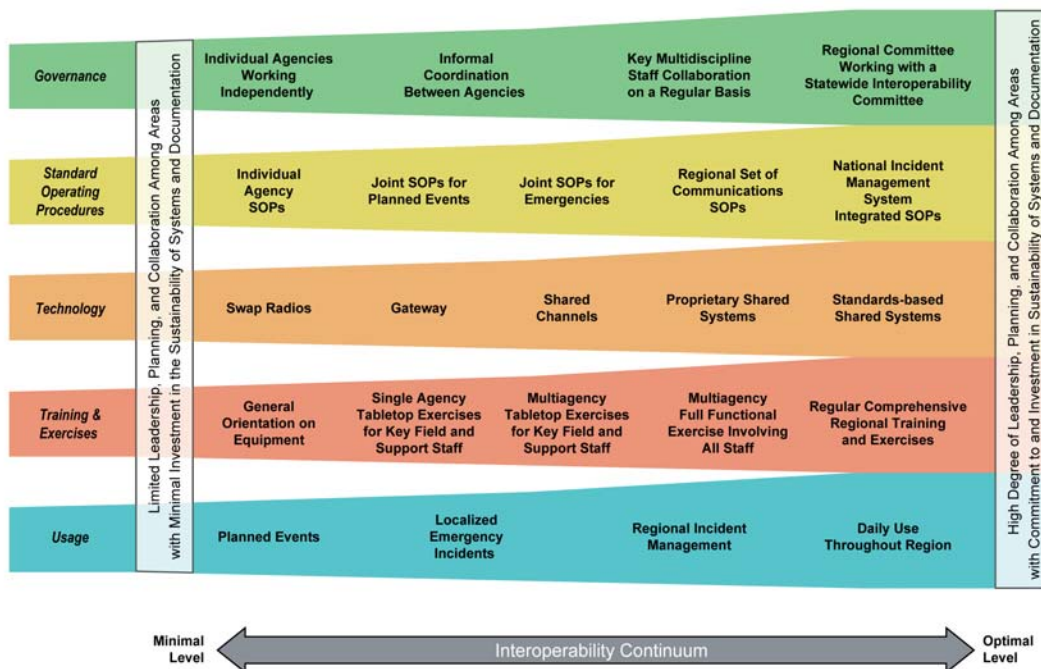
To drive progress on the Continuum and improve interoperability, public safety practitioners should:

- ➢ 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
  o 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
  - o 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
  - o The device must be capable of being powered either from vehicular power, battery power, or portable AC power sources.
  - o 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.
  - o 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.
  - o The device must have input mechanisms or modules that can support balanced or unbalanced two- or four-wire circuits.
  - o 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
  - o The device must provide local control to establish two or more talk groups of the radios/phone interfaces that are provided.
  - o 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.
  - o 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.

<u>APPENDIX J</u>

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.

<u>APPENDIX K</u>

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.

<u>**Authorized Organization Representative and Individuals**</u>

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 <u>e-Business POC</u> for assignment of user privileges.

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

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

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, **97.059**. 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 L

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 M

APPLICATION CHECKLIST

Application Checklist

The TSP applicant must complete the following:

☐ **SF-424 Grant Application with Certifications (as file attachments in Grants.gov)**
    ☐ Assurances
    ☐ Certifications Regarding Lobbying; Debarment, Suspension, and
      Other Responsibility Matters; and Drug-Free Workplace Requirement
☐ **Program Contacts (as a file attachment in Grants.gov)**
    ☐ See sample format in Appendix B
☐ **Individual Project Plan for *each* project (as a file attachment in Grants.gov):**
    ☐ See sample format in Appendix C
☐ **Detailed Budget for *each* project (as a file attachment in Grants.gov):**
    ☐ See sample format in Appendix D
    ☐ Include any project-specific M&A costs in the detailed budget for that project
    ☐ Include any general M&A costs in a separate detailed budget
☐ **DUNS Number (through Grants.gov form)**
☐ **Accounting System and Financial Capabilities Questionnaire, if applicable (as file attachment in Grants.gov)**

<u>APPENDIX N</u>

ACRONYMS AND ABBREVIATIONS

Acronyms and Abbreviations

A

AAR	After Action Report
ACH	Automated Clearing House
AFG	Assistance to Firefighter Grants
AOR	Authorized Organization Representative
ASAP	Automated Standard Application of Payments
ATA	American Trucking Associations

B

BZPP	Buffer Zone Protection Program

C

CAPR	Categorical Assistance Progress Reports
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CCR	Central Contractor Registry
CFDA	Catalog of Federal Domestic Assistance
CFR	Code of Federal Regulations
CI/KR	Critical Infrastructure/Key Resource
CIP	Critical Infrastructure Protection
CMC	Crisis Management Center
COR/COS	Carrier Operated Relay/Carrier Operated Squelch
CRWG	Comprehensive Review Working Group
CSID	Centralized Scheduling and Information Desk

D

D&B	Dun and Bradstreet
DHS	U.S. Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DOT	Department of Transportation
DUNS	Data Universal Numbering System

E

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
FY	Fiscal Year

G

G&T	Office of Grants and Training
GAN	Grant Adjustment Notice
GAO	Government Accountability Office
GMS	Grants Management System

H

HHS	U.S. Department of Health and Human Services
HSEEP	Homeland Security Exercise and Evaluation Program
HSIN	Homeland Security Information Network
HSOC	Homeland Security Operations Center
HSPD	Homeland Security Presidential Directive

I

ICP	Incident Command Post
ICS	Incident Command System
IED	Improvised Explosive Device
IP	Improvement Plan
IPP	Infrastructure Protection Program
ISAC	Information Sharing and 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
LMR	Land Mobile Radio
LOCES	Letter of Credit Electronic Certification System

M

M&A	Management and Administration
MOU	Memorandum of Understanding
MPIN	Marketing Partner Identification Number
MRA	Mutual Response Agreement

N

NIC	NIMS Integration Center
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NPG	National Preparedness Guidance
NRP	National Response Plan

	NSTS	National Strategy for Transportation Security

O

	OC	Office of the Comptroller
	OGO	Office of Grant Operations
	OIP	Office of Infrastructure Protection
	OJP	Office of Justice Programs
	OMB	Office of Management and Budget

P

	PAPRS	Phone Activated Paperless Request System
	PIN	Personal Identification Number
	POC	Point of Contact
	POETE	Planning, Organization, Equipment, Training, and Exercise
	PSTN	Public Switched Telephone Network
	PTT	Push-to-Talk
	PW	Private Wireless

R

	RAD/NUC	Radiological/Nuclear
	RDT&E	Research, Development, Test and Evaluation
	RKB	Responder Knowledge Base
	RTSS	Regional Transit Security Strategy
	RTSWG	Regional Transit Security Working Group

S

	SOP	Standard Operating Procedure
	SSA	Sector-Specific Agency
	SSP	Sector-Specific Plan

T

	TA	Technical Assistance
	TCL	Target Capabilities List
	TPIN	Trading Partner Identification Number
	TRC	Tone Remote Control
	TSA	Transportation Security Administration
	TSP	Trucking Security Program
	TSOC	Transportation Security Operations Center

U

	UASI	Urban Area Security Initiative
	USC	United States Code
	USCG	U.S. Coast Guard
	UTL	Universal Task List

V

	VOX	Voice Operated Transmit