



# **FY 2006 Homeland Security Grant Program**

**Program Guidance and Application Kit**

**December 2005**



**Homeland  
Security**

### ***Disclaimer***

*The views and opinions of authors of reference materials expressed herein do not necessarily reflect those of the United States Government.*

*Reference within this document to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government.*

*The information and statements contained within this document shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the United States Government.*

*With respect to any other information contained within non-DHS documents or reference materials referred to within this guidance, neither the United States Government nor any of its employees make any warranty, express or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose. Further, neither the United States Government nor any of its employees assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product or process disclosed; nor do they represent that its use would not infringe privately owned rights.*

## FOREWORD

On October 18, 2005, the President signed the Department of Homeland Security (DHS) Appropriations Act of 2006, providing vital funding needed to ensure the safety and security of our homeland. Through the DHS Preparedness Directorate's Office of Grants and Training (G&T) (formerly the Office of State and Local Government Coordination and Preparedness (SLGCP)), State and local organizations will receive approximately \$2.5 billion in grant funding to build capabilities that enhance homeland security.

DHS is charged with maximizing the security of our homeland. We must prioritize our efforts based on risk, and we must invest wisely to ensure timely and effective improvement. In recognition of this reality, the FY 2006 Homeland Security Grant Program (HSGP) outlines a prioritized approach to funding allocations with an emphasis on risk and need.

This year marks the first grant cycle in which we have a National Preparedness Goal to shape National Priorities and focus expenditures. This common planning framework and the tools that support it allows us as a Nation to better understand how prepared we are, how prepared we need to be, and how we prioritize efforts to close that gap.

As in previous fiscal years, the FY 2006 HSGP continues to provide funding for planning, organization, equipment, training, exercises, and management and administration to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies in all 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and the U.S. Territories. States and Territories will now have the opportunity to implement their recently updated Homeland Security Strategies and continue to improve upon existing capabilities.

The Department recognizes that implementing the National Preparedness Goal is a long-term endeavor. We remain committed to working with States and Urban Areas to build and enhance preparedness capabilities in the coming years.

The FY 2006 HSGP reflects the Department's commitment to work closely with the Nation's homeland security stakeholders in a unified national effort to address terrorist attacks, major disasters, and other emergencies and enhance the security of our homeland.



Michael Chertoff  
Secretary  
Department of Homeland Security

## Table of Contents

<b>I.</b>	<b>National Preparedness.....</b>	<b>1</b>
<b>II.</b>	<b>Program Guidance.....</b>	<b>16</b>
<b>III.</b>	<b>Eligible Applicants and Funding Availability .....</b>	<b>52</b>
<b>IV.</b>	<b>Application Kit.....</b>	<b>57</b>
<b>V.</b>	<b>Award and Reporting Requirements .....</b>	<b>63</b>
<b>VI.</b>	<b>State Homeland Security Program.....</b>	<b>69</b>
<b>VII.</b>	<b>Urban Areas Security Initiative.....</b>	<b>76</b>
<b>VIII.</b>	<b>Law Enforcement Terrorism Prevention Program .....</b>	<b>87</b>
<b>IX.</b>	<b>Metropolitan Medical Response System.....</b>	<b>94</b>
<b>X.</b>	<b>Citizen Corps Program.....</b>	<b>106</b>
	<b>Appendix A – Sample Award Package .....</b>	<b>A-1</b>
	<b>Appendix B – Investment Justification.....</b>	<b>B-1</b>
	<b>Appendix C – Memorandum of Understanding Template .....</b>	<b>C-1</b>
	<b>Appendix D – Allowable Cost Matrix.....</b>	<b>D-1</b>
	<b>Appendix E – Historical Allowable Data .....</b>	<b>E-1</b>
	<b>Appendix F – Relationship of Grant Programs to Target Capabilities.....</b>	<b>F-1</b>
	<b>Appendix G – NIMS State, Territorial and Tribal Compliance Activities .....</b>	<b>G-1</b>
	<b>Appendix H – Geospatial Guidance .....</b>	<b>H-1</b>
	<b>Appendix I – Cyber Security Guidance .....</b>	<b>I-1</b>
	<b>Appendix J – Domestic Nuclear Detection Office (DNDO) .....</b>	<b>J-1</b>
	<b>Appendix K – Public Safety Communications &amp; Interoperability guidance .....</b>	<b>K-1</b>
	<b>Appendix L – Web Resources.....</b>	<b>L-1</b>
	<b>Appendix M – Acronyms.....</b>	<b>M-1</b>
	<b>Appendix N – Index .....</b>	<b>N-1</b>

## Table of Figures

<b>Figure 1 – Target Capabilities .....</b>	<b>12</b>
<b>Figure 2 – Process Overview .....</b>	<b>14</b>
<b>Figure 3 – Relationship of Initiatives to Goals, Objectives, Investments, and Projects.....</b>	<b>B-2</b>
<b>Figure 4 – Interoperable Communications as a Priority, Capability, Strategic Goal, Initiative and Investment, and Project.....</b>	<b>B-2</b>

## Table of Tables

<b>Table 1 – FY 2006 Homeland Security Grant Program.....</b>	<b>16</b>
<b>Table 2 – Other FY 2006 Office of Grants and Training Grant Programs.....</b>	<b>17</b>
<b>Table 3 – FY 2006 Other Preparedness Grant Programs.....</b>	<b>19</b>
<b>Table 4 – FY 2005 DHS/HHS Preparedness Programs.....</b>	<b>20</b>
<b>Table 5 – POETE and the Elements of Capability .....</b>	<b>31</b>
<b>Table 6 – MMRS Jurisdictions .....</b>	<b>54</b>
<b>Table 7 – Application Checklist.....</b>	<b>57</b>
<b>Table 8 – SHSP Allowable Equipment Categories .....</b>	<b>73</b>
<b>Table 9 – UASI Allowable Equipment Categories.....</b>	<b>84</b>
<b>Table 10 – LETPP Allowable Equipment Categories .....</b>	<b>90</b>
<b>Table 11 – MMRS Allowable Equipment Categories.....</b>	<b>102</b>
<b>Table 12 – CCP Allowable Equipment Categories .....</b>	<b>110</b>
<b>Table 13 – FY 2006 Allowable Cost Matrix.....</b>	<b>D-1</b>
<b>Table 14 – Historical Planning Categories .....</b>	<b>E-1</b>
<b>Table 15 – Historical Equipment Costs .....</b>	<b>E-1</b>
<b>Table 16 – Historical Training Costs .....</b>	<b>E-2</b>
<b>Table 17 – Historical Exercise Costs .....</b>	<b>E-3</b>
<b>Table 18 – Historical Management &amp; Administrative Costs.....</b>	<b>E-3</b>
<b>Table 19 – Relationship of Grants to Target Capabilities.....</b>	<b>F-1</b>
<b>Table 20 – NIMS Implementation Matrix for States and Territories.....</b>	<b>G-4</b>
<b>Table 21 – NIMS Implementation Matrix for Tribal and Local Jurisdictions.....</b>	<b>G-15</b>
<b>Table 22 – Minimum (“no worse than”) Goals for Resolution, Accuracy, and Currency.....</b>	<b>H-3</b>
<b>Table 23 – TA for RAD/NUC Preventive Detection Programs .....</b>	<b>J-2</b>

## FY 2006 Homeland Security Grant Program (HSGP) Guidance Revisions

January 3, 2006		
Location	Section	Change
Pg. 45, 1 <sup>st</sup> Bullet under Unauthorized Exercise Costs	Chapter II: Program Guidance; Section D – Allowable Cost Guidance; Subsection D.5. – Exercises, Unauthorized Exercise Costs	Added mileage to fuel/gasoline as the only vehicle costs that are reimbursable.
Pg. 54, 2 <sup>nd</sup> Paragraph	Chapter III: Eligible Applicants and Funding Availability; Section C – Funding; Subsection C.1. – FY 2006 SHSP and LETPP Allocations	Deleted “UASI” from the first sentence. UASI will not be allocated using the USA PATRIOT Act formula
Pg. 58, 6 <sup>th</sup> Paragraph	Chapter IV: Application Kit, Section 3 – For identified UASI Urban Areas, 1 <sup>st</sup> Bullet	Replaced 2 <sup>nd</sup> sentence for clarity
Pg. 59, 1 <sup>st</sup> Paragraph	Chapter IV: Application Kit, Section 3 – For identified UASI Urban Areas, 2 <sup>nd</sup> Bullet	Replaced 2 <sup>nd</sup> sentence for clarity
Pg. 59, 3 <sup>rd</sup> Paragraph	Chapter IV: Application Kit, Section 3 – For identified UASI Urban Areas, 3 <sup>rd</sup> Bullet	Replaced 1 <sup>st</sup> sentence for clarity
Pg. 78, 1 <sup>st</sup> Paragraph	Chapter VII: Urban Areas Security Initiative; Section B – Program Requirements, Governance	Revised governance discussion related to Urban Area Working Groups (UAWG)
Pg. 79, 1 <sup>st</sup> Paragraph	Chapter VII: Urban Areas Security Initiative; Section B – Program Requirements, Defining Urban Areas	Urban Area definition requirements language updated for clarity
Pg. 79, 3 <sup>rd</sup> Paragraph, 2 <sup>nd</sup> Bullet	Chapter VII: Urban Areas Security Initiative; Section B – Program Requirements, Defining Urban Areas, 3 <sup>rd</sup> Paragraph, 2 <sup>nd</sup> Bullet	Revised language for clarity
Pg. 92, 2 <sup>nd</sup> Paragraph	Chapter VIII: Law Enforcement Terrorism Prevention Program; Section C – Authorized Program Expenditures; Subsection C.7. – Management and Administration	Deleted “UASI” and replaced it with “LETPP” in the discussion of M&A costs associated with the LETPP program

# **I. NATIONAL PREPAREDNESS**

## I. NATIONAL PREPAREDNESS

### A. The FY 2006 Homeland Security Grant Program

The FY 2006 Homeland Security Grant Program (HSGP) integrates the State Homeland Security Program (SHSP), the Urban Areas Security Initiative (UASI), the Law Enforcement Terrorism Prevention Program (LETPP), the Metropolitan Medical Response System (MMRS), and the Citizen Corps Program (CCP). This combined FY 2006 HSGP Program Guidance and Application Kit builds upon the FY 2005 HSGP to streamline efforts for States and Urban Areas in obtaining resources that are critical to building and sustaining capabilities to achieve the Interim National Preparedness Goal (the Goal) and implement State and Urban Area Homeland Security Strategies.<sup>1</sup>

Several significant changes in the HSGP and its focus are being made for FY 2006. First, this marks the first grant cycle in which the Interim National Preparedness Goal is in place to outline National Priorities and focus expenditures on building capabilities. This common planning framework and the tools that support it allow the Nation to define target levels of performance and measure progress made toward achieving them. In addition, the Department of Homeland Security (DHS) is adopting in FY 2006 a risk- and need-based approach to allocating funding for certain programs within HSGP. The aim is to allocate and apply these resources to generate the highest return on investment and, as a result, strengthen national preparedness in the most effective and efficient manner. In addition to integrating these new policy developments, the FY 2006 HSGP guidance:

- Highlights the Interim National Preparedness Goal and its applicability to the FY 2006 HSGP
- Highlights the Target Capabilities List and its applicability to the FY 2006 HSGP
- Presents overall FY 2006 HSGP policy and program requirements, including overall FY 2006 HSGP allowable costs
- Guides grantees in the application and award process for the FY 2006 HSGP
- Provides detail on the specific requirements associated with FY 2006 SHSP, UASI, LETPP, MMRS, and CCP

**The National Preparedness Goal:**

To achieve and sustain risk-based target levels of capability to prevent, protect against, respond to, and recover from major events, and to minimize their impact on lives, property, and the economy, through systematic and prioritized efforts by Federal, State, local and Tribal entities, their private and non-governmental partners, and the general public.

### B. The National Preparedness Goal

On March 31, 2005, DHS issued the Interim National Preparedness Goal (the Goal). The Goal establishes a vision for National Preparedness including National Priorities. The Target Capabilities List (TCL)

<sup>1</sup> The Emergency Management Performance Grant (EMPG) Program was included in the FY 2005 HSGP application, however in FY 2006, EMPG was released as a stand-alone application earlier in the fiscal year.



identifies 37 capabilities integral to Nation-wide all-hazards preparedness, including acts of terrorism.<sup>2</sup> The national preparedness doctrine and operational foundation provided in these documents form the basis for Federal preparedness assistance going forward. The Goal is a significant evolution in the approach to preparedness and homeland security. It presents a collective vision for national preparedness, and establishes National Priorities to guide the realization of that vision to meet the most urgent needs. The Goal is a companion document to the National Response Plan (NRP), National Incident Management System (NIMS), and the interim 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 Incidents of National Significance as defined in the NRP.<sup>[1]</sup> Additionally, the Goal will assist entities at all levels of government 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 shall be performed pursuant to the final National Preparedness Goal following its expected release soon after the FY 2006 HSGP guidance.

The Goal and the TCL are all-hazard in nature, addressing a range of major events, including terrorism and the capabilities required to address them. However, the five programs included in the HSGP do not support all elements within each capability in the TCL. A number of additional resources at different levels of government are available and should be leveraged to build and sustain capabilities. For example, the Triage and Pre-Hospital Treatment Capability of the TCL recommends sufficient numbers of certified/licensed emergency medical service (EMS) personnel; however, the costs associated with hiring those personnel are not allowable under HSGP.

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. Some capabilities fall outside the scope of HSGP funding and are the responsibility of other Federal agencies or State and local governments. 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.<sup>3</sup>

<sup>2</sup> This guidance references 37 capabilities based on the most recent draft of the TCL available at the time the guidance went to press.

<sup>3</sup> NIMS, March 2004.

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.<sup>4</sup> 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.<sup>5</sup>

**Respond:** Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. As indicated by the situation, response activities include: applying intelligence and other information to lessen the effects or consequences of an incident; increasing security and law enforcement operations; continuing investigations into the nature and source of the threat; continuing ongoing public health and agricultural surveillance and testing processes; providing immunizations; enforcing isolation or quarantine; and allowing appropriate citizen response.<sup>6</sup> 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, nongovernmental, 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.<sup>7</sup>

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 shall be modified to reflect the completion or update of assessments, and shall include benchmarks for measuring

<sup>4</sup> Homeland Security Presidential Directive (HSPD) 7, December 2003.

<sup>5</sup> The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003.

<sup>6</sup> NIMS, March 2004.

<sup>7</sup> NIMS, March 2004.

the achievement of unmet capabilities over time. Additional foreseeable changes to the documents and their implementation shall include:

- Recommendations and lessons learned from the response to Hurricane Katrina identified by the Comprehensive Review Working Group (CRWG).
- Revisions to the National Response Plan.
- Capabilities required for implementing the National Infrastructure Protection Plan.
- Capabilities required for implementing the National Strategy for Pandemic Influenza.
- Prevention tasks and capabilities identified by updated National Planning Scenarios and reflective of current Administration policies on the War on Terror.

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

## **C. 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) three overarching priorities that contribute to the development of multiple capabilities, and (B) four capability-specific priorities that build selected capabilities for which the Nation has the greatest need. 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 include:

### **C.1. Expanded Regional Collaboration**

Major events, especially terrorism, will invariably have cross-geographic consequences and impact. The Expanded Regional Collaboration Priority highlights the need for embracing partnership 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 leverage 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 critical infrastructure and key resources. The Goal establishes as a priority the embracing of regional approaches to building, sustaining, and sharing capabilities at all levels of government.

Benchmarks for implementation of this National Priority include:

- Formalize mutual aid agreements with surrounding communities and States for the purposes of sharing equipment, personnel, and facilities during emergencies.
- Exercise the execution of mutual aid agreements to identify challenges and familiarize officials with resources that are available in the region.

- Coordinate homeland security preparedness assistance expenditures and planning efforts on a regional basis to avoid duplicative or inconsistent investments.

During FY 2006 and FY 2007, DHS will continue to review progress on several ongoing regional collaboration efforts, including:

- Progress made by Urban Area Working Groups under the UASI program with regard to implementing the vision, goals, and objectives outlined in the Urban Area Homeland Security Strategies.
- Progress on Regional Transit Security Strategy Working Group structure supported by the Transit Security Grant Program (TSGP), under which State, local, Tribal, and parish leadership joined the respective transit leadership to coordinate a collective approach to managing the needs of the eligible transit grant recipients in concert with the balance of the transportation providers for that region.

## **C.2. Implement the NIMS and NRP**

Homeland Security Presidential Directive-5 (HSPD-5), “*Management of Domestic Incidents*,” mandated the creation of NIMS and NRP. The NRP establishes a comprehensive all-hazards approach to managing domestic incidents. The plan incorporates best practices and procedures from incident management disciplines – homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector – and integrates those best practices and procedures into a unified structure. The NIMS provides a consistent framework for entities at all jurisdictional levels to work together to implement the NRP and manage domestic incidents, regardless of cause, size, or complexity. To promote interoperability and compatibility among Federal, State, local, and Tribal capabilities, the NIMS includes a core set of guidelines, standards, and protocols for command and management, preparedness, resource management, communications and information management, supporting technologies, and management and maintenance of NIMS. The NRP, using the template established by the NIMS, is an all-discipline, all-hazards plan that provides the structure and mechanisms to coordinate operations for evolving or potential Incidents of National Significance. Based on the criteria established in HSPD-5, Incidents of National Significance are those high-impact events that require a coordinated and effective response by an appropriate combination of Federal, State, local, Tribal, private sector, and nongovernmental 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, Homeland Security Presidential Directive - 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 governments as appropriate.

State, local, and Tribal entities are required to become fully compliant with NIMS by the end of FY 2006 (September 30, 2006). Entities are required to meet the FY 2006 NIMS implementation requirements as a condition of receiving Federal preparedness funding assistance in FY 2007. States and Territories must establish a planning process that incorporates the appropriate procedures to ensure the effective communication and implementation of NIMS requirements across the State, including Tribes and local governments. This planning process must include a means for measuring progress and facilitate the reporting of NIMS implementation among its Tribal and local jurisdictions. Office of Grants and Training (G&T) will continue to update grantees on NIMS compliance measures as they become available.

Benchmarks for implementation of this National Priority include:

- State, local, and Tribal entities should be fully compliant with NIMS by the end of FY 2006 (September 30, 2006). As part of this compliance, States and Territories must institute the planning process called for in the September 2005 letter to Governors to ensure effective communication and implementation of NIMS requirements across the State, including Tribes and local governments.
- Progress toward the additional steps that State, Territorial, Tribal, and local entities should take during FY 2006 to become fully compliant with the NIMS, as outlined in the FY 2006 NIMS Implementation Matrices, included as Appendix G.

For FY 2007, compliance with NIMS implementation requirements will be a condition of receiving Federal preparedness funding assistance.

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

### **C.3. Implement the Interim NIPP**

The interim NIPP, published in February 2005, establishes a process for bringing together a wide range of homeland security partners at the Federal, State, local, and Tribal level to establish the organized, unified, national risk-based approach to enhance the security and mitigate the risk facing the Nation's critical infrastructure and key resources. The interim NIPP delineates roles and responsibilities for homeland security partners in carrying out these activities, while respecting the authorities, jurisdictions, and prerogatives of these partners. Importantly, the risk-based process established through the NIPP will assist authorities in determining which critical infrastructure and key resources are critical at the national level and those which are critical at the State-level, thereby establishing a baseline understanding of how Federal and State funding resources could be best leveraged to enhance security. Investments and planning to improve critical infrastructure protection must support the final NIPP following its issuance in 2006.

Infrastructure protection involves a multi-faceted understanding of the risks and vulnerabilities facing infrastructure sectors that cross geospatial boundaries. It also requires an understanding of the inter-relationships of infrastructure sectors within geospatial areas. Consequently, protecting critical infrastructure and key resources sites is a shared responsibility requiring cooperation among all levels of government – Federal, State, local, and Tribal – and the involvement of the private sector. Effective security involves plans that define, identify, and set priorities for the most critical structures and assets that are potential targets for terrorist attacks. With the inclusion of interim NIPP implementation as a National Priority, infrastructure protection efforts are a required component of both State and Urban Area Strategies and thus form a key pillar of the overarching homeland security program.

States and Urban Areas are responsible for developing and implementing a critical infrastructure protection program as a component of their overarching homeland security program. This program should engage all relevant intergovernmental coordination points (e.g., Federal, State, local, and Tribal) to ensure a comprehensive approach to critical infrastructure protection across all appropriate levels of government, across both public and private sectors, within geospatial areas, and across infrastructure sectors.

Benchmarks for implementation of this National Priority include:

- During FY 2006 States and Urban Areas should establish a critical infrastructure protection program as a component of their overarching homeland security program.
- The critical infrastructure program should engage all relevant intergovernmental coordination points (e.g., Federal, State, local, and Tribal) to ensure a comprehensive approach to critical infrastructure protection across all appropriate levels of government, across both public and private sectors, within geospatial areas, and across infrastructure sectors.

Later this year, the DHS Preparedness Directorate will release guidance for several additional grant programs supporting the protection of critical infrastructure assets.

In addition to the overarching priorities, there are four capability-specific priorities:

#### **C.4. Strengthen Information Sharing and Collaboration Capabilities**

Effective terrorism prevention, protection, response, and recovery efforts depend on timely, accurate information about the identity of the enemy, 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.

Benchmarks for implementation of this National Priority include:

- Access to the DHS Homeland Security Information Network to strengthen the real-time collaborative flow of threat information among homeland security partners.

- Access to the Department of Justice (DOJ) Law Enforcement Information Sharing Program which provides exchange services that enhance the information sharing capabilities of DOJ.
- Participation in the Joint Terrorism Task Forces led by the Federal Bureau of Investigation (FBI). The Task Forces enhance communication, coordination, and cooperation among agencies at all levels of government representing intelligence, law enforcement, defense, diplomatic, public safety, and homeland security disciplines by providing a point of fusion for terrorism intelligence.
- Participation in the Anti-Terrorism Advisory Councils led by the U.S. Attorney’s Office. These councils facilitate information sharing among law enforcement organizations at all levels of government.
- Development of State and local capabilities to gather, analyze, disseminate, and use information regarding threats, vulnerabilities, and consequences to support prevention and response efforts. DHS will issue guidance for such intelligence fusion capabilities to ensure consistent protocols and procedures across jurisdictional lines.

**C.5. Strengthen Interoperable Communications Capabilities**

The lack of interoperable wireless communication systems is an issue that continues to affect public safety agencies in communities across the country. In many cases, agencies are unable to communicate or share critical voice and data information with other jurisdictions or disciplines during major events or even day-to-day operations. Interoperable communications, 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, is a capability-specific priority. 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 (SOPs) – 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.

States and Urban Areas were to show in their updated homeland security strategy how they plan to achieve interoperability on a regional, State, or multi-State level, in support of their efforts to establish integrated regional operational systems.

In addition, all Urban Areas and select other metropolitan areas are required as part of the FY 2005 HSGP to develop and validate a Tactical Interoperable Communications Plan (TICP). The goal of the plan is to enable local public safety agencies to communicate as they prevent or respond to a CBRNE terrorist attack. The TICP leverages other Federal, State, and local interoperability efforts whenever possible to enhance the overall capacity for agencies and individuals to communicate with one another. These plans are due to G&T no later than May 1, 2006. Jurisdictions then have one year in which to validate the plan through an exercise.

More information on implementing interoperable communications can be found from the Office for Interoperability and Compatibility (OIC) SAFECOM at <http://www.safecomprogram.gov/SAFECOM/grant/default.htm>. Appendix K provides additional information on public safety communications and interoperability.

Benchmarks for implementation of this National Priority include:

- States and Urban Areas receiving FY 2006 HSGP funding must respond to the Interoperability Baseline Study survey instrument that will be disseminated in February 2006.
- Application of the Interoperability Continuum in implementation of ongoing interoperable communications initiatives in accordance with State and Urban Area Homeland Security Strategies.
- Development and validation of Tactical Interoperable Communications Plans (TICP) to enable rapid on-scene, incident-based mission critical voice communications among all emergency responder (e.g., EMS, fire and law enforcement) agencies and in support of NIMS. The TICP requirement in the FY 2005 HSGP is based on the RapidCom initiative. These plans are due to G&T no later than May 1, 2006. Jurisdictions have one year from date of submission in which to validate the plan through an exercise. New Urban Areas receiving FY 2006 UASI program funds must meet the TICP development and validation requirement. The objective end-state is to enable on-scene, incident-based mission critical voice communications in the 77 multi-jurisdictional areas subject to this FY 2005 HSGP requirement.
- By the end of 2007, each State must develop and adopt a Statewide communications interoperability plan.

#### **C.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. States and Urban Areas should continue to implement a broad range of activities, including planning,



organization, equipment, training, and exercises in an effort to build new and strengthen existing CBRNE detection, response, and decontamination capabilities.

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. Appendix J provides more information about DNDO, the program guidance, and the support DNDO will provide to State and local entities.

Benchmarks for implementation of this National Priority include:

- Acquisition and deployment of chemical/biological detection systems with a focus on broad system-wide protection for high threat, urban transit systems and major indoor sports and convention venues.
- Acquisition, consolidation, and coordinated deployment of explosive countermeasures capabilities, including explosives detection technologies for high-density venues such as transit systems, sports and special event venues, and shopping malls.
- RAD/NUC detection equipment procured with HSGP funding complies with DNDO technical guidance and/or established technical requirements, as they become available.
- Incorporation of DNDO guidance on RAD/NUC response protocols and linkages to appropriate State emergency operations centers, as it becomes available.

#### **C.7. Strengthen Medical Surge and Mass Prophylaxis Capabilities**

Effective medical surge and mass prophylaxis capabilities require embracing a multi-disciplinary and multi-jurisdictional collaborative approach. These capabilities should be supportive of integrated regional operational systems that are being established in support of the expanded Regional Collaboration priority, and demonstrate effective integration among public health, healthcare services, and other appropriate disciplines (e.g., emergency management, emergency medical services), mass transit and Regional Transit Security Working Groups to enhance evacuation planning, and surge volunteers. Much work in these areas is being funded through programs administered by the U.S. Department of Health and Human Services (HHS).

States and Urban Areas should examine how they are integrating preparedness activities across disciplines to build and maintain medical surge and mass prophylaxis capabilities across all disciplines. Building and maintaining these capabilities must leverage both G&T and HHS resources and should be a collaborative effort across the State public health and healthcare agencies. Planning documents should give specific attention to how all available

preparedness funding sources can be effectively utilized in a collaborative manner to support the enhancement of these capabilities.

State health, homeland security, and emergency management organizations are encouraged to seek out, coordinate, and collaborate with one another to better understand progress made to date and to scope future activity under this priority.

Benchmarks for implementation of this National Priority include:

- Prepare jurisdictions to provide oral medications during an event to their entire population within 48 hours via a network of points of dispensing (PODs) staffed with trained/exercised paid and volunteer staff.
- Conduct planning, training, exercises to pre-identify the staff, hospital beds, and other resources that can be deployed or used following a catastrophic event.

**C.8. National Review of Emergency Operations Plans and the Status of Catastrophic Planning**

The devastating aftermath of Hurricane Katrina focused the Nation on the importance of emergency operations planning for catastrophic incidents. As a result, in addition to the seven National Priorities outlined in the Goal, the FY 2006 HSGP adds an additional priority that emphasizes emergency operations and catastrophic planning.

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

As Hurricane Katrina demonstrated, this type of incident affects key planning components including public warning and notification, evacuation, reception and shelter (including a focus on at-risk population), logistics and resource management, isolation and quarantine, volunteer and donation management, and search and rescue. These factors drive the urgency for coordinated planning to ensure effective initial response and accelerated Federal/national assistance.

In November 2005, in response to three discrete tasks from the President and Congress, DHS initiated a national review process of emergency operations plans for all States and 75 Urban Areas. This review is examining the status of catastrophic planning, including mass evacuation planning, and is employing a two-phased approach.

- In the first phase, States and Urban Areas will complete and submit to DHS a plan review template that forms a baseline national status report of emergency operations planning. This requirement, as well as the list of Urban Areas and major cities which need to meet this requirement, was outlined in greater detail in Information Bulletin #197 released on

November 23, 2005. As this report is due to Congress in February 2006, **FY 2006 HSGP funding will be contingent upon States and Urban Areas submitting the plan review template to G&T no later than January 17, 2006. Failure to meet the deadline could adversely affect FY 2006 HSGP awards.**

- During phase two, teams of subject matter experts will be dispatched to all States and Urban Areas to review emergency operations plans in greater detail and provide technical assistance. Following phase two, DHS will provide a report to the President and Congress with recommended improvements to planning processes, policies and authorities.

## D. Capabilities-Based Planning

Implementing a common, shared approach to achieving national preparedness requires the Nation to re-orient its programs and efforts in support of the Goal and the National Priorities. The Goal establishes a vision for preparedness, identifies Target Capabilities, provides a description of each capability, and presents guidance on the levels of capability that Federal, State, local, and Tribal entities will be expected to develop and maintain. Capabilities-based planning is a process by which to achieve the Goal and the capabilities it outlines. Capabilities-based planning is defined 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.

**Figure 1 – Target Capabilities**

37 Target Capabilities	
<p style="text-align: center;"><b><u>Common</u></b></p> <ul style="list-style-type: none"> <li>•Planning</li> <li>•Communications</li> <li>•Risk Management</li> <li>•Community Preparedness and Participation</li> </ul>	<p style="text-align: center;"><b><u>Respond Mission Area</u></b></p> <ul style="list-style-type: none"> <li>•Onsite Incident Management</li> <li>•Emergency Operations Center Management</li> <li>•Critical Resource Logistics and Distribution</li> <li>•Volunteer Management and Donations</li> <li>•Responder Safety and Health</li> <li>•Public Safety and Security Response</li> <li>•Animal Health Emergency Support</li> <li>•Environmental Health</li> <li>•Explosive Device Response Operations</li> <li>•Firefighting Operations/Support</li> <li>•WMD/HazMat Response and Decontamination</li> <li>•Citizen Protection: Evacuation and/or In-Place Protection</li> <li>•Isolation and Quarantine</li> <li>•Urban Search &amp; Rescue</li> <li>•Emergency Public Information and Warning</li> <li>•Triage and Pre-Hospital Treatment</li> <li>•Medical Surge</li> <li>•Medical Supplies Management and Distribution</li> <li>•Mass Prophylaxis</li> <li>•Mass Care (Sheltering, Feeding, and Related Services)</li> <li>•Fatality Management</li> </ul>
<p style="text-align: center;"><b><u>Prevent Mission Area</u></b></p> <ul style="list-style-type: none"> <li>•Information Gathering &amp; Recognition of Indicators &amp; Warnings</li> <li>•Intelligence Analysis and Production</li> <li>•Intelligence / Information Sharing and Dissemination</li> <li>•Law Enforcement Investigation and Operations</li> <li>•CBRNE Detection</li> </ul>	
<p style="text-align: center;"><b><u>Protect Mission Area</u></b></p> <ul style="list-style-type: none"> <li>•Critical Infrastructure Protection (CIP)</li> <li>•Food &amp; Agriculture Safety &amp; Defense</li> <li>•Epidemiological Surveillance and Investigation</li> <li>•Public Health Laboratory Testing</li> </ul>	
<p style="text-align: center;"><b><u>Recover Mission Area</u></b></p> <ul style="list-style-type: none"> <li>•Structural Damage and Mitigation Assessment</li> <li>•Restoration of Lifelines</li> <li>•Economic &amp; Community Recovery</li> </ul>	

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 level. Capability-based planning necessitates the prioritization of resources and initiatives among the various capabilities. Given limited time and resources, jurisdictions will be expected to target their planning efforts 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 more advanced levels of capability may be expected of a group of jurisdictions, an entire State, or the Federal government. Consequently, incremental organizational and operational change 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 become critical elements of the new preparedness landscape.

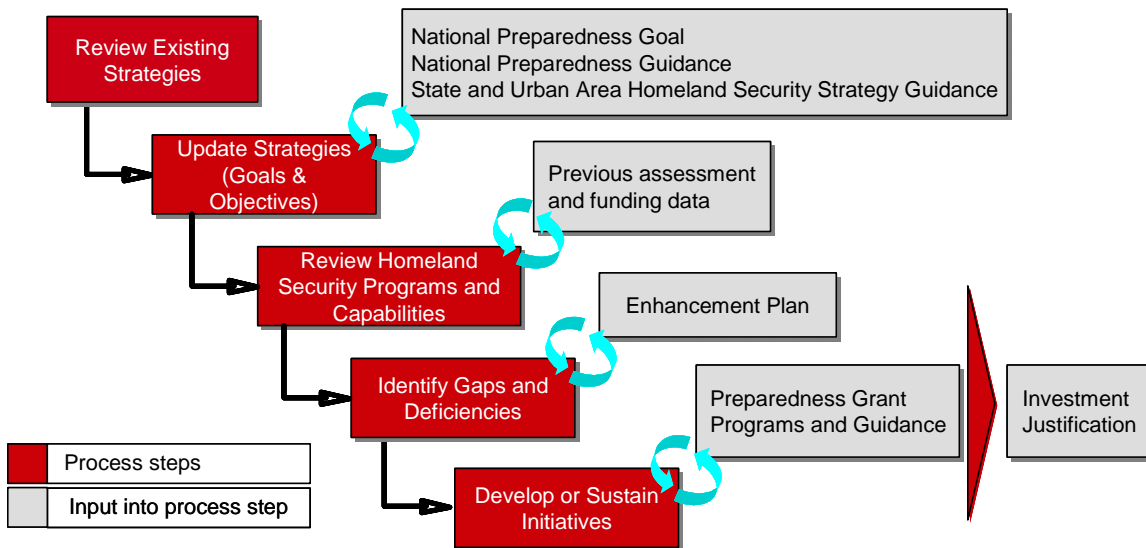
The Goal represents an all-hazards approach to preparedness. This all-hazards approach takes into consideration the special emphasis the NRP places in preparing for threats with the greatest risk of mass casualties, massive property loss, and immense social disruption, having significant national impact, requiring significant information sharing, resource coordination and assistance. As described above, catastrophic events in particular are defined in the NRP as any natural, technical, or manmade incident, including terrorism, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. All catastrophic events are considered Incidents of National Significance.

The National Planning Scenarios listed in the Goal were designed to illustrate the potential scope, magnitude, and complexity of a range of events including terrorist attacks and natural disasters. Terrorist attacks and natural or man-made disasters share numerous common characteristics. Many capabilities are common to all-hazards – whether a natural disaster, a technical accident, or a terrorist attack – including on-site incident management and search and rescue.

## **E. The National Preparedness Goal and the FY 2006 Homeland Security Grant Program**

Over the next year, focus will be placed on significantly improving or enhancing capabilities supporting the National Priorities listed in the Goal, as building blocks for a National Preparedness System. Figure 2 below shows the FY 2006 process of implementing the Goal.

**Figure 2 – Process Overview**



All States and Urban Areas were required to align existing preparedness strategies within the National Priorities by October 31, 2005. As part of the FY 2006 DHS grant process, States and Urban Areas are required to assess their preparedness needs by reviewing their existing programs and capabilities and use those findings to develop a plan and formal Investment Justification outlining major Statewide, sub-State, or inter-State initiatives for which they will seek funding.

These Statewide, sub-State, or inter-State initiatives should focus efforts on how to build and sustain programs and capabilities within and across State boundaries, while aligning with the Goal and National Priorities. Capabilities should be strategically located to maximize the return on preparedness investments, and all available funding sources (Federal, State, local, and private) should contribute to building and sustaining these capabilities.

Moving forward, DHS will continue to work closely with Federal, State, local, Tribal, private sector, and non-governmental subject matter experts to further refine the capabilities and associated targets in the TCL, and to build capabilities in the right place at the right level to minimize the impact of major events on lives, property, and the economy based on risk and need.

The FY 2006 HSGP guidance provides assistance to States and Urban Areas in applying for and leveraging Federal preparedness assistance from DHS, HHS, and other Federal agencies to enhance national preparedness by closing capability gaps and maintaining existing levels of capability. The FY 2006 HSGP is one of the primary sources of assistance for implementing the Goal and achieving and sustaining 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.

## **II. PROGRAM GUIDANCE**

## II. PROGRAM GUIDANCE

### A. Overview

The following section highlights important guidance, policy, and coordination requirements, as well as a broad discussion of allowable costs applicable across all programs through the FY 2006 HSGP. Applicants should pay close attention to the language in this section as this year’s HSGP guidance has been adjusted to reflect the new strategic context of the Goal and the National Priorities.

The FY 2006 HSGP continues the streamlined approach employed in FY 2005 with the inclusion of multiple grant programs in a single solicitation. This consolidation helps ensure that all available funding is leveraged for maximum impact. The integration of these programs also strengthens the coordination across the various programs and encourages regional preparedness efforts in support of implementing the Goal.<sup>8</sup> State and Urban Area Homeland Security Strategies were recently updated to reflect the Goal, and will continue to serve as the overarching guide for homeland security efforts as the Goal is finalized. These strategy updates represent an important first step in transitioning to the common framework for building, sustaining, and improving national preparedness for a broad range of threats and hazards that is envisioned in the Goal. While developing the application for the FY 2006 HSGP, grantees are encouraged to look across all available support and assistance programs and leverage all available funding and resources from multiple sources wherever possible.

Table 1 outlines the programs included in FY 2006 HSGP and the homeland security mission areas each program supports. In addition, Appendix G illustrates in greater detail how each grant program relates to the Goal and the TCL.

**Table 1 – FY 2006 Homeland Security Grant Program**

FY 2006 HSGP	Program Overview	Goal Mission Area
<p><b>State Homeland Security Program (SHSP)</b></p>	<p>SHSP supports the implementation of the State Homeland Security Strategy to address the identified planning, equipment, training, and exercise needs for acts of terrorism. In addition, SHSP supports the implementation of the National Preparedness Goal, NIMS, and the NRP.</p>	<p>Common Activities, Prevent, Protect, Respond, Recover</p>
<p><b>Urban Areas Security Initiative (UASI)</b></p>	<p>UASI funds address the unique planning, equipment, training, and exercise needs of high threat, high density Urban Areas, and assist them in building an enhanced and sustainable capacity to prevent, protect against, respond to, and recover from acts of terrorism.</p>	<p>Common Activities, Prevent, Protect, Respond, Recover</p>

<sup>8</sup> As used in this document, the term “regional” refers to multi-State or sub-State geographic areas that function as regions (e.g., the National Capital Region) and is not a reference to any Federal regions.

FY 2006 HSGP	Program Overview	Goal Mission Area
<p><b>Law Enforcement Terrorism Prevention Program (LETPP)</b></p>	<p>LETPP focuses upon the prevention of terrorist attacks and provides law enforcement and public safety communities with funds to support the following activities: intelligence gathering and information sharing through enhancing/establishing fusion centers; hardening high value targets; planning strategically; continuing to build interoperable communications; and collaborating with non-law enforcement partners, other government agencies and the private sector.</p>	<p>Common Activities, Prevent</p>
<p><b>Metropolitan Medical Response System (MMRS) Program</b></p>	<p>MMRS funds support MMRS jurisdictions to further enhance and sustain an integrated, systematic mass casualty incident preparedness program that enables a first response during the first crucial hours of an incident. The program prepares jurisdictions for response to the range of mass casualty incidents, including CBRNE, and agriculture to epidemic outbreaks, natural disasters and large-scale hazardous materials incidents.</p>	<p>Common Activities, Prevent, Respond, Recover</p>
<p><b>Citizen Corps Program (CCP)</b></p>	<p>The Citizen Corps mission is to actively involve all citizens in hometown security through personal preparedness, training, exercises, and volunteer service. CCP funds support Citizen Corps Council efforts to engage citizens in all-hazards prevention, protection, response, and recovery.</p>	<p>Common Activities, Prevent, Protect, Respond, Recover</p>

In addition to the programs outlined in the FY 2006 HSGP, Table 2 outlines other programs also funded by G&T but not included in this guidance.

**Table 2 – Other FY 2006 Office of Grants and Training Grant Programs**

FY 2006 Program	Program Overview	Goal Mission Area
<p><b>Emergency Management Performance Grant (EMPG) Program</b></p>	<p>The EMPG program gives States the opportunity to structure individual emergency management programs based on needs and priorities for strengthening their emergency management capabilities, while addressing issues of national concern. States have the flexibility to develop systems that encourage the building of partnerships which include government, business, volunteer, and community organizations.</p>	<p>Common Activities, Protect, Respond, Recover</p>
<p><b>Buffer Zone Protection Program (BZPP)</b></p>	<p>BZPP provides funding for enhanced security of select critical infrastructures and assets. The intent of the program is to establish Buffer Zone Plans which are intended to help local law enforcement and emergency responders develop preventive measures around high priority infrastructure targets.</p>	<p>Common Activities, Prevent, Protect</p>



FY 2006 Program	Program Overview	Goal Mission Area
<b>Transit Security Grant Program (TSGP)</b>	The TSGP provides funding to support security enhancements for intracity passenger rail transportation and other security measures. The program addresses three transit modalities: rail transit, intracity bus transit, and ferry systems.	Common Activities, Prevent, Protect
<b>Port Security Grant Program (PSGP)</b>	The PSGP funds owners and operators of ports, terminals, U.S. inspected passenger vessels and ferries, as well as port authorities and State and local agencies to improve security for operators and passengers through physical security enhancements. The program strives to create a sustainable, risk-based effort for the protection of critical infrastructure from terrorism or any other incidents that would cause major disruption to commerce and significant loss of life.	Common Activities, Prevent, Protect
<b>Intercity Bus Security Grant Program (IBSGP)</b>	The IBSGP provides financial assistance to owners/operators of fixed route, intercity bus services, and special needs charter buses to improve security for operators and passengers. The program strives to create a sustainable effort for the protection of critical infrastructure terrorism or any other incidents that would cause major loss of life and severe disruption.	Common Activities, Prevent, Protect
<b>Intercity Passenger Rail Security Grant Program (IPRSGP)</b>	The IPRSGP provides financial assistance to Amtrak for the protection of critical infrastructure and preparedness activities related to terrorism or any other incidents.	Common Activities, Prevent Protect
<b>Assistance to Firefighters Grant (AFG) Program</b>	The purpose of the AFG program is to enhance the safety of the public and firefighters with respect to fire and fire-related hazards. The primary goal of the AFG Program’s Fire Prevention and Safety Grant is to reach high-risk target groups in order to mitigate the high incidences of death and injuries. Additionally, the program continues to include funding for the Firefighter Safety Research and Development. For further information contact the AFG Helpdesk at 1-866-274-0960, or look online at <a href="http://firegrantsupport.com">http://firegrantsupport.com</a>	Common Activities, Prevent, Respond,

Table 3 points to other grant programs throughout the Federal government which States can leverage for preparedness needs.

**Table 3 – FY 2006 Other Preparedness Grant Programs**

FY 2006 Program	Program Overview	Goal Mission Area
<p><b>National Bioterrorism Hospital Preparedness Program (NBHPP) Health Resources and Services Administration (HRSA), (HHS)</b></p>	<p>The purpose of the NBHPP is to prepare hospitals and supporting healthcare systems, in collaboration with other partners, to deliver coordinated and effective care to victims of terrorism and other public health emergencies. Cooperative agreement funds may be used for activities that include increasing surge capacity, which encompasses beds, personnel, pharmaceuticals, Personal Protective Equipment, decontamination capacity, isolation capacity and interoperable communications, as well as the enhancement of EMS services, competency based training, and exercises.</p>	<p>Common Activities, Respond</p>
<p><b>Bioterrorism Training and Curriculum Development Program (BTCDP), (HRSA), (HHS)</b></p>	<p>BTCDP provides support to health professions schools, health care systems, and other educational entities to equip a workforce of healthcare professionals to address emergency preparedness and response issues. The program consists of two discrete foci: (1) provision of continuing education for practicing health care providers; and (2) curriculum development and enhancement and training in health professions schools.</p>	<p>Common Activities, Respond</p>
<p><b>Public Health Emergency Preparedness Cooperative Agreement, Centers for Disease Control and Prevention (CDC), (HHS)</b></p>	<p>The purpose of the Division of State and Local Readiness' cooperative agreement program is to upgrade and integrate State and local public health jurisdictions' preparedness for and response to terrorism and other public health emergencies with Federal, State, local, and Tribal governments, the private sector, and Non-Governmental Organizations (NGOs). These emergency preparedness and response efforts are intended to support the NRP and the NIMS. Activities included in the cooperative agreement are designed to develop emergency-ready public health Departments.</p>	<p>Common Activities, Respond</p>
<p><b>Federal Emergency Management Agency (FEMA) Mitigation Grants (DHS)</b></p>	<p>The Pre-Disaster, Flood, and Hazard Mitigation Programs provides States and local governments financial assistance to implement measures that will permanently reduce or eliminate future damages and losses from natural hazards through safer building practices and improving existing structures and supporting infrastructure.</p>	<p>Common Activities, Protect, Recover</p>
<p><b>Edward Byrne Memorial Justice Assistance Grant Program (JAG), Department of Justice (DOJ)</b></p>	<p>The JAG Program is a partnership among Federal, State, and local governments to create safer communities. The Bureau of Justice Assistance may award grants for use by States and units of local government to improve the functioning of the criminal justice system and enforce State and local laws that establish offenses similar to those in the Federal Controlled Substances Act. Grants also may be used to provide assistance (not compensation) to victims of these offenders.</p>	<p>Common Activities, Protect, Respond</p>
<p><b>Homeland Security-Agricultural Grant, Department of Agriculture (USDA)</b></p>	<p>The purpose of the Homeland Security – Agriculture Grant is to provide funding to protect the food supply and agricultural production, protect USDA facilities and other agricultural infrastructure; and protect USDA staff and manage emergency preparedness.</p>	<p>Common Activities, Protect</p>

FY 2006 Program	Program Overview	Goal Mission Area
<b>Hazardous Materials Emergency Preparedness Grant Program (HMEP), Department of Transportation (DOT)</b>	The HMEP grant program is intended to provide financial and technical assistance as well as national direction and guidance to enhance State, Territorial, Tribal, and local hazardous materials emergency planning and training. The HMEP grant program distributes fees collected from shippers and carriers of hazardous materials to Local Emergency Planning Committees (LEPCs) for hazmat planning and to emergency responders for hazmat training.	Common Activities, Prevent, Protect

## B. Policy

### B.1. Integrating Preparedness Assistance

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

This opportunity is especially pertinent to the implementation of preparedness grant programs in DHS and HHS. In FY 2005, DHS and HHS made available approximately \$3.9 billion in grant and cooperative agreement funds to States and local jurisdictions to assist in building and sustaining national preparedness through several major grant programs, including:

**Table 4 – FY 2005 DHS/HHS Preparedness Programs**

Program Title	Sponsoring Agency	FY 2005 Funding
Homeland Security Grant Program	Office for Domestic Preparedness, DHS	\$2.5 billion
Public Health Emergency Preparedness Cooperative Agreement	Centers for Disease Control and Prevention, HHS	\$862.0 million
National Bioterrorism Hospital Preparedness Program	Health Resources and Services Administration, HHS	\$491.0 million
Bioterrorism Training and Curriculum Development Program	Health Resources and Services Administration, HHS	\$25.0 million

These grant programs target distinct but related homeland security stakeholders at the State and local levels. For example, the State Homeland Security Program within HSGP cuts across all of the capabilities in the TCL, while the Law Enforcement Terrorism Prevention Program focuses specifically on the capabilities related to prevention efforts. Likewise, CDC’s and HRSA’s emergency preparedness programs center on a number of capabilities related to health and medical efforts.

Using the Goal and the corresponding structure of the TCL as the foundation, State and local homeland security, public safety, and public and private health organizations can continue to build the framework that connect them to support the overall homeland security program. Appendix G maps the above programs to each of the Target Capabilities in an effort to emphasize areas of overlap among the programs as well as any unique focus areas of each program.

To emphasize the criticality of a coordinated approach to the management and application of these funding streams, DHS and HHS have established a Federal Preparedness Grant Program Steering Committee to strengthen the alignment of each agency's respective grant programs both with each other and within the new context of the Goal. Through this committee, DHS and HHS are working to align their programs and develop common language and analytical tools while maintaining the discreet focus areas of each program.

States should examine how they are integrating preparedness activities across disciplines and agencies. In FY 2006, States must implement a cohesive planning framework that builds and implements homeland security initiatives that leverage both DHS and HHS resources as well as other Federal and State resources. In addition to DHS and HHS resources, grantees and subgrantees should consider preparedness assistance programs from other Federal agencies including the USDA, DOJ, and DOT. Specific attention should be paid to how all available preparedness funding sources can be effectively utilized in a collaborative manner to support the enhancement of capabilities throughout the State.

In FY 2005, G&T, CDC, and HRSA encouraged the integration of disciplines through a Senior Advisory Committee to coordinate Federal assistance programs including G&T, CDC, HRSA, and other Federal entities providing homeland security assistance. This requirement remains in place in FY 2006 and underscores the importance that DHS and HHS stress to grantees and subgrantees in taking a holistic approach to implementing their strategic homeland security goals and objectives by considering all available support and assistance programs, regardless of the source.<sup>9</sup>

States are encouraged to broaden membership of the Senior Advisory Committee to include membership from additional disciplines, associations, and regional working groups.

---

<sup>9</sup> The membership of the Senior Advisory Committee must, at a minimum, include the following State officials directly responsible for the administration of Office of Grants and Training grants and CDC and HRSA cooperative agreements: the State Administrative Agency (SAA), HRSA Program Director, HRSA Bioterrorism Hospital Coordinator, and CDC Program Director. In addition, program representatives from the following entities should be members on the committee: State Homeland Security Advisor (if this role is not also the SAA); State Emergency Management Agency Director; State Public Health Officer; State Public Safety Officer (and SAA for Justice Assistance Grants, if different); State Court Official; State EMS Director; State Trauma System Manager; State Citizen Corps POC; United States Coast Guard Area Command or Captain of the Port; Senior Members of the Regional Transit Security Working Group, Senior Security Officials from Major Transportation Systems; and the Adjutant General.

## **B.2. Effective State Homeland Security Programs**

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

The State homeland security program should provide a strategic and management framework to integrate and ensure consistency among the full range of program-related activities and operational plans and procedures. The State homeland security program should work to achieve and sustain risk-based target levels of capability to prevent, protect against, respond to, and recover from catastrophic events and acts of terrorism in order to minimize the impact on lives, property, and the economy.

## **B.3. State and Urban Area Homeland Security Strategies**

For FY 2006, State and Urban Area Homeland Security Strategies will continue to provide the overarching strategic vision for the implementation of State and Urban Area homeland security programs. States and Urban Areas were recently required to update their strategies to bring the strategies into alignment with the National Priorities included in the Goal. Updated State and Urban Area Homeland Security Strategies continue to provide the context for the evaluation of preparedness programs and capabilities within and across State boundaries. In the development of the FY 2005 Regional Transit Security Strategies mass transit systems were aligned to their respective Urban Area and State Strategies in order to collaborate on a vision for transportation security. This collaborative approach will continue under the FY 2006 Transit Security Grant Program.

## **B.4. Coordination Requirements**

### ***Citizen Coordination***

State Administrative Agencies (SAAs) must coordinate State and Urban Area citizen awareness and participation activities with those State agencies currently responsible for the administration of Citizen Corps activities. Citizens are a critical component in securing the homeland. In order to have a prepared and protected community and Nation, all citizens must be educated, practiced, and trained on how to prepare for and respond to emergencies, including natural disasters and potential terrorist attacks. Through Citizen Corps and the *Ready* campaign, DHS is helping individuals and communities become better prepared. These programs engage the public and encourage them to prepare for emergencies and thus are a critical part of a better prepared America.

In support of this mission, all SHSP, UASI, LETPP, CCP, and MMRS award recipients are to work with their State and local Citizen Corps Councils to more fully engage citizens through the following:

- **Awareness and outreach to inform and engage the public:** Educate the public on personal, family and business preparedness measures, alert and warning systems, and State and local emergency plans. Encourage the public to take actions to prepare themselves, their families and their businesses via a range of communication channels and community venues, including schools when appropriate.
- **Expand plans and task force memberships to address citizen participation:** Develop or revise State and local plans, such as Emergency Operations Plans (EOPs), to integrate citizen/volunteer resources and participation, and include advocates for increased citizen participation in task forces and advisory councils.
- **Include citizens in training and exercises:** Provide emergency preparedness and response training for citizens, improve training for emergency responders to better address special needs populations, and involve citizens in all aspects of emergency preparedness exercises, including planning, implementation, and after action review.
- **Develop or expand programs that integrate citizen/volunteer support for the emergency responder disciplines:** Develop or expand the Citizens Corps Programs (Volunteers in Police Service (VIPS), Medical Reserve Corps (MRC), Community Emergency Response Teams (CERT), Neighborhood Watch, and Fire Corps), activities of the Citizen Corps affiliates, and ad hoc opportunities for citizens to support emergency responders year-round and during a disaster.

A listing of current State Citizen Corps POCs is available by visiting <http://www.citizencorps.gov/councils/> and selecting “State Citizen Corps POC List.” In support of the goals and objectives outlined in the current Homeland Security Strategies and as strategies are revised, States must include an integrated approach to engaging citizens in preparedness, training, exercises, and volunteer support for emergency responders through Citizen Corps Councils. States are encouraged to fully leverage HSGP resources to accomplish this integration.

### ***Private Sector Coordination***

States and Urban Areas should collaborate with the private sector to leverage private sector initiatives, resources, and capabilities, as permitted by applicable laws and regulations. Since critical infrastructure is often privately-owned and operated, enhancing public/private partnerships will help identify and advocate opportunities for coordination within communities. In addition, Citizen Corps Councils at all levels should work with and include representatives from the private sector as appropriate.

### ***Transit and Port Security Coordination***

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

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

States and Urban Areas are strongly encouraged to support the RTSWG and the Area Maritime Security Committees as they are integral to the achievement of regional collaboration for transportation security. For more information on maritime security issues, refer to the National Strategy for Maritime Security which was released on September 20, 2005, and is available at <http://www.whitehouse.gov/homeland/maritime-security.html>. The National Strategy for Transportation Security, which will provide a national, in-depth transportation security approach is expected to be released within the year.

### ***Emergency Medical Services Coordination***

Grantees should work closely to engage the EMS community in preparedness efforts. While G&T does not mandate how much money should be allocated to any particular discipline, Congress has raised concerns about how much funding is reaching the EMS community. As a result, Congress directed G&T in FY 2006 to evaluate how much funding is given to EMS providers and to require an explanation from any State not providing at least ten percent of its grant funding to EMS providers. States should be prepared to provide an explanation supporting EMS funding decisions to their Preparedness Officers upon request.

## **B.5. Information Technology**

### ***National Information Exchange Model***

DHS, the DOJ, and their associated domains released the National Information Exchange Model (NIEM 0.1) in October 2005. The NIEM 0.1 establishes a single standard Extensible Markup Language (XML) foundation for exchanging information between DHS, DOJ, and supporting domains, such as Justice, Emergency Management, and Intelligence. The base technology for the NIEM is the Global JXDM. The NIEM will leverage both the extensive Global JXDM reference model and the comprehensive Global JXDM XML-based framework and support infrastructure. The intended uses of this initial release are:

- To introduce NIEM to the broad NIEM stakeholder community within government and industry.
- To provide the NIEM model and schemas as a base for creating exchange messages for the initial pilot projects that will validate and augment the standard.
- To allow information technology and standards experts and users to provide feedback on the standard.
- To begin to identify additional Universal, Common, and Domain-Specific components that could be added to future versions of the standard.

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

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

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

### ***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, coordinate and track emergency assets, enhance 911 capabilities, understand event impacts, accurately estimate damage, locate safety zones for quarantine or detention, and facilitate recovery.

Appendix H contains additional guidance on geospatial issues. Authorized equipment for geospatial homeland security purposes (including hardware, software, and data) appear primarily in the *Information Technology* category of the Authorized Equipment List (AEL).

### ***Homeland Security Information Network (HSIN)***

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

DHS is requiring all State, regional, local, and Tribal entities using FY 2006 HSGP funding in support of information sharing and intelligence fusion and analysis centers to use the HSIN web-based system as the backbone for communication and collaboration with their member agencies



and the HSOC. The use of the HSIN system will enable participants in these information sharing and intelligence fusion and analysis centers to access intelligence data from multiple systems, irrespective of their platform or programming language. Participants are also encouraged to use HSIN to conduct data queries and to exchange information and reports with the HSOC on a regular basis, in accordance with appropriate State and/or local reporting procedures.

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

### ***Cyber Security***

*The National Strategy to Secure Cyberspace* notes that critical infrastructure within the United States comprises public and private institutions across a range of sectors, including agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is the nerve system that connects these sectors. Cyberspace itself is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow critical infrastructure to work. Functioning of cyberspace is essential to the economy and national security.

Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from the Nation, including the Federal, State and local governments, the private sector, and the public at large. In recognition of the importance of cyber security initiatives and the critical role States and local jurisdictions play in keeping cyberspace secure, G&T has included an annex on cyber security issues to assist grantees in developing and implementing critical cyber security efforts through FY 2006 HSGP funding.

### ***GSA's Cooperative Purchasing Program***

The U.S. General Services Administration (GSA) offers an efficient and effective procurement tool for State and local governments to purchase information technology products and services to fulfill homeland security and other needs. The GSA Schedules (also referred to as the Multiple Award Schedules and the Federal Supply Schedules) are long-term, indefinite delivery, indefinite quantity, government-wide contracts with commercial firms of all sizes. The Cooperative Purchasing program allows for State and local governments to purchase from Schedule 70 (the Information Technology Schedule) and the Consolidated Schedule (containing IT Special Item Numbers) **only**. Cooperative Purchasing is authorized by Federal law and was enacted when Section 211 of the E-Government Act of 2002 amended the Federal Property and Administrative Services Act.

Under this program, State and local governments have access to over 3,000 GSA Schedule contractors who have voluntarily modified their contracts to participate in the Cooperative Purchasing program. The U.S. General Services Administration provides a definition of State and local governments as well as other vital information under the frequently asked questions section on its website at [www.gsa.gov/cooperativepurchasing](http://www.gsa.gov/cooperativepurchasing). The term “State and local governments” does not include contractors of, or grantees of, the Federal, State, or local governments not otherwise named in the approved list of entities.

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

## C. Overarching Program Guidance

### C.1. Period of Performance

The period of performance for all programs within HSGP is 24 months from the date of award. Any unobligated funds will be deobligated by G&T at the end of this period. Extensions to the period of performance will be considered only through formal requests to G&T with specific and compelling justifications as to why an extension is required.

### C.2. Pass-Through Requirements

**SHSP, UASI, LETPP:** Each State shall make no less than 80 percent of the total grant program amount available to local units of government, including identified Urban Areas within 60 days of the receipt of funds. Any UASI funds retained by the State must be used to directly support the designated Urban Areas in the State.

**MMRS:** In States with MMRS jurisdictions, SAAs should pass 100 percent of the MMRS program funding allocation to their MMRS jurisdiction(s). For MMRS jurisdictions within multiple States, each SAA involved should pass-through 100 percent of the funding to the designated fiduciary/coordinating entity. However, States may retain up to 20 percent of the MMRS program funding allocation to facilitate strategy assessment and capability integration between the State and the MMRS jurisdictions. Any funds retained by the State must be documented in a written agreement between the SAA and Chair of the MMRS Steering Committee(s).

**CCP:** There are no minimum pass-through requirements for CCP. States are, however, expected to work with county or parish, local, and/or Tribal Citizen Corps Councils to expend funds in a manner that supports local efforts to educate, train, and involve citizens. If the State chooses to subgrant funds to a local unit of government, the recipient must have an existing Citizen Corps Council or establish a Citizen Corps Council as a condition of receiving the funding. In FY 2006, States should consider allocating CCP funds to the highest risk jurisdictions within the State. In future fiscal years, DHS may require allocation of CCP funds to be made in a similar

manner.

### ***Territorial Pass-Through Requirements***

Due to the unique nature of the Territorial governments in Guam, American Samoa, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands, no pass-through requirements will be applied to those Territories. However, these Territories are expected to take into account the needs of local communities prior to making funding distribution decisions.

### ***Memorandum of Understanding (MOU) Requirements***

For any HSGP programs involving pass-through of funds, the State may retain some or all of the local unit of government or Urban Area's allocation of grant funds for expenditures made by the State on behalf of the local unit of government or Urban Area. This may occur only if requested in writing by that local unit of government or Urban Area. States holding grant funds on behalf of local units of government or Urban Areas must enter into a formal MOU with the local unit of government or Urban Area specifying the amount of funds to be retained by the State and the intended use of funds.

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

Any new MOU request must be initiated by the local unit of government or Urban Area. States are encouraged, but not required, to submit these MOUs to their G&T Preparedness Officer for review to ensure compliance. A final, executable copy of the MOU will be kept on file with the SAA and be made available to DHS upon request. A model is available in Appendix C.

### **C.3. Drawdown of Funds**

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

These guidelines state that subgrantees are required to promptly, but at least quarterly, remit interest earned on advances to:

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

The subgrantee may keep interest amounts up to \$100 per year for administrative expenses for all Federal grants combined. Please consult the G&T Office of Grant Operations (OGO)

Financial Guide and applicable OMB Circular for additional guidance. Although advance drawdown requests may be made, State grantees remain subject to the interest requirements of the Cash Management Improvement Act (CMIA) and its implementing regulations at 31 C.F.R. Part 205. Interest under CMIA will accrue from the time Federal funds are credited to a State account until the time the State pays out the funds or transfers the funds to a subgrantee.

#### **C.4. Administrative Guidance**

##### ***Freedom of Information Act (FOIA)***

G&T recognizes that much of the information submitted in the course of applying for funding under this program, or provided in the course of its grant management activities, may be considered law enforcement sensitive or otherwise important to national security interests. This may include threat, risk, and needs assessment information, and discussions of demographics, transportation, public works, and industrial and public health infrastructures. While this information under Federal control is subject to requests made pursuant to the Freedom of Information Act, 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. Applicants are encouraged to consult their own State and local laws and regulations regarding the release of information, which should be considered when reporting sensitive matters in the grant application, needs assessment and strategic planning process. Applicants may also consult their G&T Preparedness Officer regarding concerns or questions about the release of information under State and local laws.

Grantees should be familiar with the regulations governing Protected Critical Infrastructure Information (6 C.F.R. Part 29) and Sensitive Security Information (49 C.F.R. Part 1520), as these designations may provide additional protection to certain classes of homeland security information.

##### ***Compliance with Federal Civil Rights Laws and Regulations***

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

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

benefits of or subjected to discrimination under any program or activity receiving Federal financial assistance.

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

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

Grantees are required to comply with several Federal civil rights laws, including Title VI of the Civil Rights Act of 1964, as amended. These laws prohibit discrimination on the basis of race, color, and religion, national origin, and sex in the delivery of services. National origin discrimination includes discrimination on the basis of limited English proficiency. To ensure compliance with Title VI, grantees are required to take reasonable steps to ensure that LEP persons have meaningful access to their programs. Meaningful access may entail providing language assistance services, including oral and written translation, where necessary. Because grantees are required to provide meaningful access to LEP persons in their programs and activities, grantees are encouraged to consider the need for language services for LEP persons served or encountered both in developing their proposals and budgets and in conducting their programs and activities. Reasonable costs associated with providing meaningful access for LEP individuals are considered allowable program costs. For additional information, see <http://www.lep.gov>.

***Integrating Individuals with Disabilities into Emergency Planning***

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

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

Further information can be found at the Disability and Emergency Preparedness Resource Center at [www.dhs.gov/disabilitypreparedness](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 HSGP grant expenditures should be mindful of Section 504 of the Rehabilitation

Act of 1973 that prohibits discrimination based on disability by recipients of Federal financial assistance.

### D. Allowable Costs Guidance

The Goal identifies six elements of capability that support the building and sustaining of capabilities, which are consistent with NIMS. These newly outlined elements of capability track closely with the five allowable cost categories traditionally used in G&T grant programs (planning, organization, equipment, training, and exercises, oftentimes referred to collectively as POETE). In addition to these programmatic allowable costs, HSGP also allows for personnel costs, as well as management and administrative costs. Table 5 below crosswalks the elements of capability from the Goal and the HSGP allowable cost categories in order to demonstrate the alignment between these categories.

**Table 5 – POETE and the Elements of Capability**

POETE Framework	Elements of Capability Outlined in the Goal	Element of Capability as Defined in the Goal
Planning	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	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	Equipment and Systems	Major items of equipment, supplies, facilities, and systems that comply with relevant standards necessary to perform assigned missions and tasks.
Training	Training	Content and methods of delivery that comply with relevant training standards necessary to perform assigned missions and tasks.
Exercises	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.
	Personnel (Element added in the Goal)	Paid staff who meet required qualification and certification standards necessary to perform assigned missions and tasks.

It is important to note that the elements of capability explicitly include personnel costs. Within the FY 2006 HSGP, personnel costs are generally not allowable except for specific purposes outlined within the overall HSGP program guidance below as well as in the individual program discussions.

Specific information on each program’s allowable costs is provided in the appropriate individual section included later in this guidance document. A crosswalk of allowable costs across grant

programs can be found in Appendix D. The following pages outline global allowable costs guidance applicable to all programs included in the HSGP.

**D.1. Planning**

Planning activities are central to SHSP, UASI, LETPP, MMRS, and CCP. Accordingly, States and Urban Areas may use FY 2006 HSGP funds for planning efforts that enable States and Urban Areas to prioritize needs, build capabilities, update preparedness strategies, allocate resources, and deliver preparedness programs across disciplines (e.g., law enforcement, fire, EMS, public health, behavioral health, public works, agriculture, information technology, and citizen preparedness) and levels of government. The planning process should address emergency operations plans and protocols for addressing major events and program planning for the successful implementation and management of each State’s homeland security program. Examples of allowable planning costs are addressed in each program’s individual section.

**D.2. Organization (UASI and LETPP only)**

States and Urban Areas may use FY 2006 UASI and LETPP funds to support select organization activities. States and Urban Areas must justify proposed expenditures of UASI or LETPP funds to support organization activities within their Investment Justification submission using historical data and other analysis to substantiate their proposals. No more than 25 percent of the gross amount of the allocation for these programs may be used for operational expenses and overtime costs for the three (3) operational activities noted below.

1. Operational overtime costs associated with increased security measures at critical infrastructure sites during DHS-declared periods of heightened alert.

**UASI:** Up to 25 percent of FY 2006 funds may be used in UASI jurisdictions.

- Of this amount, up to 10 percent may be used for costs incurred during Code Yellow or Orange.
- The remaining 15 percent may be used for costs incurred only during Code Orange.
- Operational overtime costs incurred at National Special Security Events (NSSEs) in UASI jurisdictions, as designated by the Secretary of Homeland Security, are also allowed.
- States with UASI jurisdictions can use funds retained at the State level to reimburse eligible operational overtime expenses incurred by the State (up to a maximum of 25 percent of the State share of the UASI grant). However, those activities must directly support increased security measures enacted in the UASI jurisdictions. States should be judicious in the use of Federal grant funds when protecting critical infrastructure and should leverage public/private partnerships. States should also consider the use of private assets in the protection of private facilities.

**LETPP:** Up to 25 percent of FY 2006 LETPP funds may be used for costs incurred during Code Orange. Costs associated with **border protection activities only** are also eligible at Code Yellow, provided that those activities are conducted in accordance with

previous guidance issued in Information Bulletin #135 and outlined below. These activities must be coordinated with U.S. Customs and Border Protection (CBP).

In support of these efforts for enhanced capabilities of detecting, deterring, disrupting, and preventing acts of terrorism, costs eligible for reimbursement under this policy are identical to those deemed allowable under previous Code Orange alerts. Therefore, subject to the conditions stated above, States and local governments may use FY 2006 UASI and LETPP funds to support select operational expenses associated with increased security measures at critical infrastructure sites in the following authorized categories:

- Backfill and overtime expenses for staffing State or local emergency operations centers (EOCs).
- Hiring of contracted security for critical infrastructure sites.
- Public safety overtime.
- National Guard deployments to protect critical infrastructure sites, including all resources that are part of the standard National Guard deployment package.
- Increased border security activities in coordination with CBP, as outlined in Information Bulletin #135.<sup>10</sup>

Consumable costs, such as fuel expenses, are *not allowed* except as part of the standard National Guard deployment package.

2. Overtime costs are allowable for personnel to participate in information, investigative, and intelligence sharing activities specifically related to homeland security. This includes activities such as anti-terrorism task forces, Joint Terrorism Task Forces (JTTF), Area Maritime Security Committees (as required by the Maritime Transportation Security Act of 2002), and Terrorism Early Warning (TEW) groups.
3. Grant funds may be used for the hiring of new staff and/or contractors to serve as intelligence analysts to enable information/intelligence sharing capabilities. In order to be hired as an Intelligence Analyst, staff and/or contractor personnel must have successfully completed training to ensure baseline proficiency in *intelligence analysis and production*. Furthermore, costs associated with hiring new intelligence analysts are allowable only for the period of performance of the FY 2006 UASI and LETPP programs. Upon close-out of the FY 2006

---

<sup>10</sup> Proposed operational activities should emphasize those measures that will increase border security in direct coordination with CBP personnel. State, local, and Tribal law enforcement personnel may provide increased enforcement presence by generally increasing their patrol presence at the border; by providing additional traffic control support at the border and at border patrol traffic checkpoints; and by enhancing their participation in the Integrated Border Enforcement Teams. This policy does not result in a change or extension of Federal authority to State, Tribal, or local law enforcement agencies to enforce Federal immigration laws. If Federal immigration violations are encountered, consistent with current practices, State, local, and Tribal agencies may refer those violations to CBP authorities for appropriate action. No funds may be obligated or drawn down in support of these activities without HQ-CBP approval of operational plans and without submission to and approval by G&T of budget detail worksheets. State, local, and Tribal law enforcement agencies shall not use this funding to supplant routine patrol and law enforcement operations or activities in order to perform other activities not directly related to providing an enhanced law enforcement presence.



grants, States and Urban Areas shall be responsible for supporting the sustainment costs for those intelligence analysts.

The International Association of Law Enforcement Intelligence Analysts' (IALEIA) Educational Standard # 7 (page 14 of the IALEIA Analytic Standards booklet) provides standards on the categories of training needed for intelligence analysts. These include subject-matter expertise, analytic methodologies, customer-service ethics, information handling and processing skills, critical thinking skills, computer literacy, and objectivity and intellectual honesty. Successful completion the following courses satisfies the intelligence analyst training requirement:

- Intelligence Analyst Training Program (FLETC)
- Foundations of Intelligence Analysis Training (International Association of Law Enforcements Intelligence Analysis)

Additional courses are being identified and will be shared as soon as possible. *A certificate of completion of such training must be on file with the SAA and should be made available to Preparedness Officers upon request upon the hiring of personnel.*

### D.3. Equipment

Allowable equipment categories for FY 2006 HSGP are listed on the web-based AEL on the Responder Knowledge Base (RKB), which is sponsored by G&T and the National Memorial Institute for the Prevention of Terrorism (MIPT) at <http://www.rkb.mipt.org>.

The FY 2006 HSGP AEL is housed on the RKB along with separate listings for the FY 2005 AEL and the Fall 2005 Standardized Equipment List (SEL). In some cases, items on the SEL are not allowable under FY 2006 HSGP or will not be eligible for purchase unless specific conditions are met. In addition, some new items that are eligible under FY 2006 HSGP are not available for purchase with FY 2005 funds. During the course of FY 2006, G&T will highlight significant updates to the AEL in real time on the RKB. These updates will be noted in a change log posted on the main page of the AEL within the RKB. In addition, the RKB will also be posting a new section on the website that links AEL items to the 37 capabilities included in the TCL.

Significant changes to several personal protective equipment standards are expected during FY 2006. Grantees should refer to the notes included in each equipment item entry within the AEL for additional information on these changes and their impact on allowability.

The 21 allowable categories of equipment under FY 2006 HSGP are listed in Appendix D. Any questions or suggestions concerning the eligibility of equipment not addressed in the AEL should be directed to the appropriate G&T Preparedness Officer. The "Other Authorized Equipment" category on the AEL contains a number of equipment-related costs, such as sales tax, leasing of space, installation, and maintenance. Grantees should refer to that section for specific guidance. Unless otherwise specified, maintenance costs/contracts for authorized equipment purchased using FY 2006 HSGP funding or acquired through G&T's Homeland Defense Equipment Reuse

(HDER) Program are allowable. Additional guidance and considerations for interoperable communications issues, including equipment, is included in Appendix K.

As required by the FY 2006 DHS Appropriations Conference Report, if States plan to purchase interoperable communications equipment, they must certify to G&T that they have an implementation plan for the equipment that includes governance structures, policies, procedures, training, and planned exercises to ensure that key elements of planning, governance, and training are addressed before the equipment is procured. These requirements for interoperable communications projects can be addressed through the Investment Justification that States will submit as part of the FY 2006 HSGP application process.

#### **D.4. Training**

States, Territories, and Urban Areas should use HSGP funds to enhance the capabilities of State and local emergency preparedness through the development of a State homeland security training program. Allowable training-related costs under G&T grant programs include the establishment, support, conduct, and attendance for training programs specifically identified under the SHSP, UASI, LETPP, MMRS, and CCP grant programs within existing training academies, universities or junior colleges.

These training programs include, but are not limited to, CBRNE terrorism and catastrophic events, cyber/agriculture/food security, and citizen preparedness. The target audience for training courses includes emergency prevention, protection, response, and recovery personnel, emergency managers and public/elected officials within the following disciplines: fire service, law enforcement, emergency management, emergency medical services, hazardous materials, public works, public health, health care, public safety communications, governmental administrative, and the private sector. The target audience also includes personnel representing functional areas such as critical infrastructure/ key resource protection including cyber, agriculture, and food security. The homeland security training program may also include training for citizens in preparedness, prevention, response skills, and volunteer activities and should be coordinated through State and local Citizen Corps Councils. The training program should be self sustaining, following the model outlined for in section D.5 for exercises.

Training conducted using HSGP funds should address a performance gap identified through an After Action Report/Improvement Plan or build a capability that will be evaluated through an exercise. Exercises should be used to provide responders the opportunity to demonstrate and validate skills learned in training as well as to identify training gaps. Any advanced training or training gaps should be identified in the AAR/IP and addressed in the training cycle of State or Urban Area activities.

#### ***Allowable Training Costs***

Allowable training-related costs include, but are not limited to, the following:

1. Costs to develop, deliver, and evaluate training, to include costs related to administering the training; planning, scheduling, facilities, materials and supplies, reproduction of materials, and equipment.

2. Overtime and backfill costs associated with attendance at G&T-sponsored and/or approved training courses and programs.
3. Costs associated with the certification and re-certification of instructors.
4. Travel costs (e.g., airfare, mileage, per diem, hotel) are allowable as expenses by employees who are on travel status for official business related to approved training.
5. Hiring of full or part-time staff or contractors/consultants. Full or part-time staff may be hired to support training-related activities. Payment of salaries and fringe benefits must be in accordance with the policies of the State or unit(s) of local government and have the approval of the State or awarding agency, whichever is applicable. Such costs must be included within the funding allowed for program management personnel expenses, which must not exceed 15% of the total allocation as specified in section D.6.

***Training Information Reporting System (“Web-Forms”)***

Web-Forms is an electronic form/data management system built to assist the SAA and the State/Territory Training Point of Contact (TPOC) with the reporting of training information not provided by G&T. Most noticeable this year is the movement of Web-Forms from a public domain to a SAA/TPOC Toolkit located in the administrative side of [www.firstrespondertraining.gov](http://www.firstrespondertraining.gov), a username/password protected site. Usernames and passwords, along with detailed instructions on new features and usage, will be provided to each SAA and TPOC.

Some new Web-Form features for FY 2006 include:

- Ability of the SAA/TPOC to track sponsored courses through G&T review process.
- Ability of the SAA/TPOC to view submitted Web-Forms.
- Ability to view the approved State (State/Territory sponsored) and Federal (Federal sponsored) course catalogs.
- Ability to participate in G&T Cooperative Training Outreach Program (CO-OP).

***Definitions***

- **G&T Provided Training:** those courses or programs developed for and/or delivered by institutions and organizations funded directly by G&T.
- **Training Not Provided by G&T:** those courses that are either State sponsored or Federal sponsored, coordinated and approved by the SAA or TPOC, and fall within the G&T mission scope to prepare State and local personnel to prevent, protect against, respond to, and recover from acts of terrorism or catastrophic events.
- **State Sponsored Courses:** those courses developed for and/or delivered by institutions or organizations other than Federal entities or G&T and are sponsored by the SAA or TPOC.
- **Approved State Sponsored Course Catalog:** listing of State/Territory sponsored courses that fall within G&T mission scope and have been approved through G&T course review and approval process.

- **Federal Sponsored Courses:** those courses developed for and/or delivered by institutions funded by Federal entities other than G&T.
- **Approved Federal Sponsored Course Catalog:** listing of Federal-sponsored courses that fall within G&T mission scope, and have been approved through G&T course review and approval process. This catalog was previously known as the “Eligible Federal Terrorism Training Course Catalog.”

***Attending Training Not Provided by G&T (State or Federal Sponsored Courses)***

States, Territories, and Urban Areas are not required to request approval from G&T for personnel to attend training not provided by G&T (State or Federal Sponsored courses) provided that the training is coordinated and approved by the SAA or TPOC and falls within G&T mission scope of preparing State and local personnel to prevent, protect against, respond to, and recover from acts of terrorism or catastrophic events. States, Territories, and Urban Areas are required, after attendance, to submit information through the SAA or TPOC via the Web-Forms on all training not provided by G&T but supported with G&T funds. This information will consist of course title, course description, mission area, level of training, the training provider, the date of the course, the number and associated disciplines of the individuals, and the sponsoring jurisdiction. Access to Web-Forms will be accomplished through the SAA/TPOC toolkit located in the administrative portion of [www.firstrespondertraining.gov](http://www.firstrespondertraining.gov). States Territories, and Urban Areas intending to use G&T funds to support attendance at training not provided by G&T must ensure these courses:

1. Fall within G&T mission scope to prepare State and local personnel to prevent, protect, respond to, and recover from acts of terrorism and catastrophic events.
2. Build additional capabilities that a) support a specific training need identified by the State, Territory, and Urban Area, and b) comport with the State, Territory, or Urban Area Homeland Security Strategy.
3. Address specific tasks and/or competencies articulated in G&T’s *Emergency Responder Guidelines* and the *Homeland Security Guidelines for Prevention and Deterrence*.
4. Address specific capabilities and related tasks articulated in the Target Capabilities List (TCL) and the Universal Task List (UTL).
5. Comport with all applicable Federal, State, and local regulations, certifications, guidelines, and policies deemed appropriate for the type and level of training.

In support of the continuing efforts to build common catalogs of approved training not provided by G&T, the SAA/TPOC will be allowed three deliveries of the same course within a State/Territory before the course is required to go through G&T course review and approval process. Additional course deliveries will be authorized during the review period. However, if the course is disapproved as part of the process, no additional G&T funds can be dedicated to attending the course.

### *State and Federal Sponsored Course Catalogs*

Courses approved by G&T will be added to either the approved State Sponsored Course Catalog or the Federal Sponsored Course Catalog. Courses identified within these catalogs may be attended on an unlimited basis within any State/Territory as long as the training is coordinated and approved by the SAA/TPOC. A full description of the G&T Course Development, Review, and Approval Process can be found at <http://www.ojp.usdoj.gov/odp/training.htm>.

At any time, the SAA/TPOC (for State sponsored courses) or the Federal Agency POC (for Federal sponsored courses) may request the addition of a course to the corresponding approved catalog by submitting the associated Web-Form (i.e., Request for addition to the Approved State Sponsored Catalog) for review. If it is determined that the proposed course meets the above listed criteria, the providing entity (SAA/TPOC or Federal Agency POC) will be invited to submit the Course Review and Approval Request Form along with all supporting training materials.

Required supporting training materials to be included are:

1. **Mission Area:** The submitting entity will identify the mission area(s) of the course and materials submitted. The following mission areas will be used as defined in the Goal and supported by the TCL: Prevent, Protect, Respond, Recover, and/or common.
2. **Target Audience:** The submitting entity will identify the target audience(s) of the course and materials submitted. The following list of disciplines should be used: fire service, law enforcement, emergency management, emergency medical services, hazardous materials, public works, public health, health care, public safety communications, governmental administrative, cyber security, agriculture security, food security, private security, and citizens.
3. **Level of Training:** The submitting entity for all response area training will identify the level(s) of training of the course and materials submitted. Each submission must be identified as Awareness, Performance-Defensive (OSHA Operations), Performance-Offensive (OSHA Technician), OSHA Specialist, Planning/Management (OSHA Command) Levels. More detailed information on these levels can be found at <http://www.ojp.usdoj.gov/odp/training.htm> or <http://www.osha.gov>. **Note:** G&T has received numerous requests from stakeholders to realign training levels with OSHA's standard terminology. The G&T Training Division has taken this request under advisement and will coordinate these efforts in FY 2006 with its Federal, State, local, and Tribal partners to ensure that training requirements complement regulatory requirements to the greatest extent possible.
4. **Program of Instruction (POI)/Syllabus:** The POI or syllabus is an outline, or matrix, of the course content. It addresses the scope of the training, course learning objectives, duration of the training (broken down by module, session, or lesson), resource requirements, instructor to student ratio, and an evaluation strategy. These items are not all-inclusive, but are the minimum categories that should be addressed.

5. **Training Support Package (TSP):** The TSP is all of the materials associated with the delivery of the training course. Items that should be in the TSP are as follows:
  - a. **Instructor Guide/Instructor Outline/Instructor Lesson Plans.** The published instructor material that contains course text and special instructor notes that provides the information to deliver the material.
  - b. **Participant Manual/Guide/Workbook.** The published student material that contains the supporting information in booklet, electronic, or handout form that the participant has available for reference.
  - c. **Audio/Visual Support Materials.** Any audio/visual components that are part of any learning module, session, lesson or that supports the overall training being delivered.
  - d. **Special Support Materials.** Any descriptions of practical exercises, table-top exercises, hands-on exercises or other material that supports the learning objectives.
  
6. **Module/Session/Lesson Content:** Training courses should be designed based on a building block approach. Each sub-component in the course should be titled as a module, session, or lesson. Regardless of the title, each module, session, or lesson, should have a Lesson Administration Page (LAP) that outlines the following:
  - a. **Scope Statement.** A brief description of the content of the module, session, or lesson.
  - b. **Terminal Learning Objectives (TLO).** An action verb statement that outlines what the student is expected to learn or be capable of performing at the conclusion of the module, session, or lesson. There should be only one TLO per module, session, or lesson.
  - c. **Enabling Learning Objectives (ELO).** Enabling learning objectives are the incremental learning objectives that support the TLO. There should be at least one ELO per module, session, or lesson. Each ELO must be a measurable performance statement that enables the student to demonstrate achievement of the TLO.
  - d. **Resource List.** A listing of the resources needed to successfully accomplish the module, session, or lesson.
  - e. **Instructor to Student Ratio.** The instructor to student requirement for successful presentation of the material (e.g., 1:25).
  - f. **Reference List.** A listing of all reference materials used to develop the module, session, or lesson. This information may also be included as a bibliography.

- g. Practical Exercise Statement.** This describes any exercises associated with the module, session, or lesson.
- h. Evaluation Strategy.** This defines the strategy to used to evaluate the module, session, or lesson (e.g., written and/or performance tests or assessments).

For further information on developing courses using the instructional design methodology and tools that can facilitate the process, SAAs and TPOCs are encouraged to review the G&T Strategy for Blended Learning and access the responder training development system available at [www.firstrespondertraining.gov](http://www.firstrespondertraining.gov).

Several broad categories of courses will automatically qualify for support using G&T funds and as they become identified will be included in the list of approved training not provided by G&T. Examples of these broad categories are:

1. All NIMS training approved by the NIMS Integration Center (NIC).
2. All Incident Command System (ICS) training offered through the National Fire Academy (NFA) and the Emergency Management Institute (EMI).

G&T funds must be used to supplement, not supplant, existing funds that have been appropriated for the same purpose. G&T will conduct periodic reviews of all State, Territory, and Urban Area training funded by G&T. These reviews may include requests for all course materials (POI/TSP) and physical observation of, or participation in, the funded training. If these reviews determine that courses are outside the scope of this guidance, grantees will be asked to repay grants funds expended in support of those efforts.

Training conducted with G&T support must demonstrate linkage to a Target Capability and be applicable to the State, Territory, Urban Area, or homeland security strategy.

States and territories are encouraged to conduct an annual Training and Exercise Plan Workshop to identify key priorities and major events over a multi-year time frame and align training and exercises in support of those priorities. A Multi-year Training and Exercise Plan will be produced from a Training and Exercise Plan Workshop to include the State’s training and exercise priorities, associated training and exercise capabilities, and a multi-year training and exercise schedule. Further guidance concerning the Multiyear Training and Exercise Plan can be found the exercises discussion in section D.5.

***Office of Grants and Training Cooperative Training Outreach Program (CO-OP)***

New to this year’s HSGP is the G&T Cooperative Training Outreach Program (CO-OP), which is a voluntary program designed to increase flexibility for States and Territories while enhancing G&T’s training delivery capability and complementing the current Training Partner pool. Funding from previous fiscal years **may** be used to support a State, Territory, or Urban Area’s implementation of this program.

Through the CO-OP, the SAA will have the authority to adopt various G&T sponsored and certified programs for delivery by institutions within their State and local jurisdictions, and

designate institutions as recognized providers for the identified standardized curriculum. The CO-OP will provide a training infrastructure for implementation and institutionalization that addresses the challenges experienced by State, local, and Tribal jurisdictions related to TTT efforts. G&T recognizes existing capabilities of State/local Fire and Police Academies, Universities and Community Colleges, and other certified or approved institutions to deliver identified G&T sponsored and certified training programs through TTT methods. For more detailed information on the CO-OP, please see Information Bulletin #193, dated October 20, 2005.

#### **D.5. Exercises**

Exercises conducted with G&T support (grant funds or direct support) must be managed and executed in accordance with the Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP Volumes I-III contain guidance and recommendations for designing, developing, conducting, and evaluating exercises. HSEEP Volume IV provides sample exercise materials. All four volumes can be found on the HSEEP website at <http://hseep.dhs.gov>.

#### ***NIMS Compliance***

Exercises conducted using HSGP funding must be NIMS compliant.

#### ***Training and Exercise Plan Workshop***

In previous guidance States have been required to conduct an annual Exercise Plan Workshop and out of that workshop, develop and implement a Multi-year Exercise Plan. In addition to this exercise requirement, States are now encouraged to coordinate exercises with training courses and produce a Multi-year Training and Exercise Plan. As part of the capabilities-based planning process, this workshop will now be modified to address training in addition to exercises. Through the Training and Exercise Plan Workshop, States will identify training and exercise priorities which align to their Homeland Security Strategies and map to the 37 Target Capabilities identified as part of the implementation of the Goal. The Training and Exercise Plan Workshop will provide States the opportunity to identify key priorities and major events over a multi-year timeframe and align training and exercises in support of those priorities.

A Multi-year Training and Exercise Plan will be produced from a Training and Exercise Plan Workshop and submitted to G&T through G&T's Secure Portal located at <https://odp.esportals.com>. The Training and Exercise Plan will include the State's training and exercise priorities (based on the homeland security strategy and previous year improvement plans), associated training and exercise capabilities, and a multi-year training and exercise schedule (to be updated annually and resubmitted to G&T within 60 days of the Workshop). The schedule should reflect all exercises that are being conducted throughout the State, not just those that are sponsored by G&T. All scheduled exercises must be entered through G&T Secure Portal (<https://odp.esportals.com>).

The Training and Exercise Plan should employ a cycle of activity that includes training and exercises of increasing levels of complexity. A cycle of exercises will, at a minimum, include the completion of at least one discussion-based exercise, followed by at least one operations-based exercise building upon the lessons learned from the discussion-based exercise. For example, a jurisdiction may conduct a workshop to develop a plan, followed by a tabletop exercise to



validate the plan using a hypothetical scenario, ending with a functional exercise where the plan is put into operational use. This exercise cycle must be completed within the two year grant period. The training cycle will follow a building block approach which identifies, for each State priority, the related capability(ies), the population requiring training, the level of training required (awareness, operations, technician, specialist, or command) and the desired time frame for training to occur.

States are also encouraged to develop a schedule within the Training and Exercise Plan that takes into consideration anticipated training needs of the State for at least the immediate year, with exercises being timed to provide responders the opportunity to utilize training received. This combined schedule should also ensure that training and exercises complement each other. The purpose of this combined approach is to coordinate training and exercises for the State, and to ensure the scheduling of both training and exercises which are based on national and State priorities and their associated capabilities as found in the TCL. An example of a combined Multi-year Training and Exercise Plan can be found at the HSEEP Website or G&T Secure Portal. Further guidance concerning Training and Exercise Plan Workshops can be found in the HSEEP Volumes.

Exercises within the Training and Exercise Plan must be conducted in accordance with the guidance provided by HSEEP, with enough time between the exercises to create an After Action Report/Improvement Plan (AAR/IP) in order to ensure that the exercises address lessons learned, and improvements are made to training, equipment, and plans. It is up to the State, in consultation with their Exercise Manager, to determine the starting point within the cycle, as well as the appropriate mix and range of exercises necessary to meet this requirement. Information on types of exercises, as well as exercise design and development and document templates can be found in HSEEP Volumes I-IV, located at <http://hseep.dhs.gov>.

### ***Exercise Scenarios***

In previous years, SHSP/UASI funding was focused strictly on enhancing capabilities to prevent, respond to, or recover from CBRNE, agriculture, and cyber terrorism incidents. In FY 2006, the scope of this program is being broadened to include not only terrorism but also natural and technological disasters (with the exception of LETPP-funded exercises which must be terrorism only). If conducting a natural or technological disaster exercise, the scenario must be catastrophic in scope and size. As defined by the NRP, a catastrophic incident is any natural, technical, or manmade incident, including terrorism, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. Catastrophic incidents can result in sustained national impacts over a prolonged period of time; almost immediately exceed resources normally available to State, local, Tribal, and private-sector authorities in the impacted area; and significantly interrupt governmental operations and emergency services to such an extent that national security could be threatened.

If a State or jurisdiction chooses to conduct an exercise involving a natural and/or technological disaster scenario, that exercise(s) must be reflected on the State's Multi-year Training and Exercise Plan. The catastrophic exercises should also be planned far enough in advance to involve the Federal, State, Tribal, and local stakeholders that would normally participate in a real world event.

Exercise planners may use the National Planning Scenarios as a reference or model for scenario design, or as a planning tool to help conceptualize the magnitude of threats facing a jurisdiction. *However, it is not necessary for jurisdictions to replicate the National Planning Scenarios in their exercises.* Rather, planners should use the tasks and capabilities, derived from the National Planning Scenarios, to design objectives and a scenario tailored to the exercising jurisdiction.

The scenarios used in SHSP and UASI -funded exercises must focus on validating existing capabilities (e.g., training, equipment, plans) and must be large enough in scope and size to exercise several tasks and warrant involvement from multiple jurisdictions and disciplines. Exercise scenarios should also be based on the State or Urban Area Homeland Security Strategy and Multi-year Training and Exercise Plan.

Grantees are allowed flexibility to develop exercise scenarios that apply to their jurisdiction within these planning assumptions. Grantees that need further clarification on exercise-related issues, including planning, conduct, and scenarios, should consult with their G&T Exercise Manager for assistance and/or approval.

#### ***Models, Simulations and Games (MS&G)***

Grantees who wish to expend funds on models, simulations, or games (MS&G) must consult with “Review of Models, Simulations, and Games for Domestic Preparedness Training and Exercising, Volume III,” which provides an overview and analysis of existing models, simulations and games. Grantees can also consult with the MS&G Decision Support System which automates the aforementioned report into a searchable database. Both the report and system are available through the HSEEP website.

#### ***Special Event Planning***

If a State or Urban Area will be hosting an upcoming special event (e.g., Super Bowl, G-8 Summit), or they anticipate that they will apply to be a venue for a future Top Officials (TOPOFF) exercise, they should plan to use SHSP or UASI funding to finance training and exercise activities in preparation for that event. States should include all confirmed or planned special events in the Multi-year Training and Exercise Plan.

#### ***Integration of Training with Exercises***

Exercises conducted using grant funds should provide a venue for first responders to utilize training received through G&T and other entities. Exercises should be used to provide responders the opportunity to demonstrate skills learned in training as well as to identify training gaps. Any advanced training or training gaps should be identified in the AAR/IP and addressed in the training cycle of State and Urban Area activities.

#### ***Exercise Evaluation***

All exercises will be performance-based and evaluated. An After Action Report/Improvement Plan (AAR/IP) will be prepared and submitted to G&T following every exercise, regardless of type or scope. Some exercises, such as seminars and workshops may not require the same level of analysis as a tabletop, drill, functional or full-scale exercise, but they should still produce an AAR/IP.

AAR/IPs, which must conform to the HSEEP format, should capture objective data pertaining to exercise conduct and must be developed based on information gathered through Exercise Evaluation Guides (EEGs) found in HSEEP Volume IV. These EEGs will allow evaluators to assess responder performance within the Universal Task List, which collectively achieves the capabilities of the Target Capabilities List. Based on the observations and assessed criteria denoted in the EEGs, the AAR/IP will include recommendations, action items for improvement, identify educational opportunities for involved disciplines, assigned due dates and responsibilities, and an overall assessment of the exercise. The EEGs and AAR/IP are currently being updated to reflect the TCL/UTL. These revisions should be finalized by 1st quarter 2006. In the interim of these revisions, the current HSEEP EEGs and AAR/IP template should be utilized.

AAR/IPs must be provided to G&T within 60 days following completion of each exercise (see HSEEP Volume IV for sample AAR/IP template). Currently, these AAR/IPs can be submitted through the G&T Secure Portal. However, G&T is working with other agencies to develop an online AAR/IP reporting system.

In order to leverage assessments to ensure the gathering of objective exercise-based data, States are encouraged to form Cadres of Evaluators. These Cadres should be comprised of peers in the areas being evaluated, and would be available to evaluate exercises occurring throughout the State.

### ***Self-Sustaining Exercise Programs***

States are expected to develop a self-sustaining State Homeland Security Exercise and Evaluation Program. This may include, for example: hiring dedicated exercise program staff, awareness seminars on HSEEP, attending exercise training courses, and maintaining a system to track the completion and submission of AAR/IPs from exercises (including costs associated with meeting with local units of government to define procedures).

Training on the use and implementation of HSEEP is being offered to States and Territories, and includes independent study and mobile course curriculum on the creating of a Multi-year Training and Exercise Plan, as well as the planning, conduct, and evaluation of exercises.

### ***Citizen Participation in Exercises***

Citizen participation in exercises is encouraged, to include backfilling non-professional tasks for first responders deployed on exercise, administrative and logistical assistance with exercise implementation, and providing simulated victims, press, and members of the public. Citizen participation in exercises should be coordinated with local Citizen Corps Council(s).

### ***Allowable Exercise Costs***

Allowable exercise-related costs include:

- **Funds Used to Design, Develop, Conduct and Evaluate an Exercise** – Includes costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, travel, and documentation.
- **Hiring of Full or Part-Time Staff or Contractors/Consultants** – Full or part-time staff may be hired to support exercise-related activities. Payment of salaries and fringe

benefits must be in accordance with the policies of the State or unit(s) of local government and have the approval of the State or the awarding agency, whichever is applicable. Such costs must be included within the funding allowed for program management personnel expenses, which must not exceed 15% of the total allocation as specified in section D.6. The services of contractors/consultants may also be procured to support the design, development, conduct and evaluation of exercises. The applicant's formal written procurement policy or the Federal Acquisition Regulations (FAR) must be followed.

- **Overtime and Backfill** – Overtime and backfill costs associated with the design, development and conduct of exercises are allowable expenses.
- **Travel** – Travel costs (e.g., airfare, mileage, per diem, hotel) are allowable as expenses by employees who are on travel status for official business related to the planning and conduct of the exercise project(s).
- **Supplies** – Supplies are items that are expended or consumed during the course of the planning and conduct of the exercise project(s) (e.g., copying paper, gloves, tape, non-sterile masks, and disposable protective equipment).
- **Implementation of HSEEP** – This refers to costs related to developing and maintaining a self-sustaining State Homeland Security Exercise and Evaluation Program which is modeled after the national HSEEP.
- **Other Items** – These costs include the rental of space/locations for exercise planning and conduct, rental of equipment (e.g., portable toilets, tents), food, refreshments, gasoline, exercise signs, badges, etc.

#### *Unauthorized Exercise Costs*

Unauthorized exercise-related costs include:

- Reimbursement for the maintenance and/or wear and tear costs of general use vehicles (e.g., construction vehicles) and emergency response apparatus (e.g., fire trucks, ambulances). The only vehicle cost that is reimbursable is fuel/gasoline and mileage.
- Equipment that is purchased for permanent installation and/or use, beyond the scope of exercise conduct (e.g., electronic messaging signs).

#### **D.6. Personnel**

Hiring, overtime, and backfill expenses are allowable under this grant only to perform programmatic activities deemed allowable under existing guidance. (See individual program guidance sections for more information on allowable activities.) Supplanting, however, is not allowed.

Up to 15% of programmatic spending may be used to support the hiring of full or part-time personnel to conduct program activities that are allowable under the FY 2006 HSGP (i.e., planning, training program management, exercise program management, etc). Grantees may request that DHS issue a waiver to increase that ceiling. Waiver decisions are at the discretion of DHS and will be considered on a case-by-case basis. The ceiling on personnel costs does not apply to contractors, and is in addition to eligible M&A costs and eligible hiring of intelligence analysts. Grantees may hire staff only for program management functions not operational duties.

Hiring planners, training program coordinators, exercise managers, and grant administrators fall within the scope of allowable program management functions. Grant funds may not be used to support the hiring of sworn public safety officers to fulfill traditional public safety duties. For example, a local, uniformed, law enforcement patrol officer cannot be hired using grant dollars to perform routine local law enforcement patrol duties. As another example, firefighters cannot be hired using grant dollars to perform routine fire service duties or serve on hazardous materials units.

Grantees are permitted to hire or laterally move existing public safety officers to new positions that support allowable HSGP program management functions. In the case of lateral transfers, grant funds may be used to support only those positions that are allowable under FY 2006 HSGP program guidance.

In addition, positions created and funded through G&T grants may continue to be supported with future year funding provided that the position is dedicated to the same or similar purposes allowable under applicable G&T program guidance.

The following are definitions for the terms as used in this section:

- **Overtime** – These expenses are the result of personnel who worked over and above their normal scheduled daily or weekly work time in the performance of G&T-approved activities.
- **Backfill** – Also called “Overtime as Backfill,” these expenses are the result of personnel who are working overtime in order to perform the duties of other personnel who are temporarily assigned to G&T-approved activities outside their core responsibilities. Neither overtime nor backfill expenses are the result of an increase of Full-Time Equivalent (FTEs) employees.
- **Hiring** – State and local entities may use grant funding to cover the salary of newly hired personnel that are undertaking allowable G&T program activities. This may also include new personnel that are hired to fulfill duties as a result of existing personnel being reassigned full-time to other G&T-approved activities. Hiring will always result in a net increase of FTEs.
- **Supplanting** – Replacing a currently budgeted full-time position with one or more full-time employees.

#### **D.7. Management and Administrative (M&A) Costs**

All programs within FY 2006 HSGP have allowable M&A costs for both the State as well as the local unit of government, Urban Area, or designated subgrantee. No more than 5 percent of the total amount allocated to the State for programs within FY 2006 HSGP may be retained at the State level and used for M&A purposes. These State M&A funds must be included when accounting for the total funds retained by the State. States may apply M&A funds from all five programs under the FY 2006 HSGP to M&A costs accrued under any of the FY 2006 HSGP programs. For example, States can use M&A funds from SHSP to support M&A costs associated with MMRS.

In addition, local jurisdiction subgrantees may retain and use up to 3 percent of their subaward from the State for local M&A purposes. States may pass through a portion of the State M&A allocation to local subgrantees in order to supplement the 3 percent M&A allocation allowed on subgrants. However, no more than 5 percent of the total subaward may be expended by subgrantees on M&A costs.

**D.8. Construction and Renovation**

Use of HSGP funds for construction and renovation is generally prohibited except as outlined below. Such construction and renovation shall be strictly limited and allowable only when it is a necessary component of a security system at critical infrastructure facilities.

- CCP and MMRS funds may not be used for any type of construction or renovation.
- Project construction and renovation not exceeding \$1,000,000 is allowable, as deemed necessary by the Executive Director, G&T, under SHSP, UASI, and LETPP. These program funds may be used for construction and renovation projects only when those projects specifically address enhanced security at critical infrastructure facilities. The following actions and improvements are considered to constitute construction or renovation, and must follow the approval process outlined below.
  - Construction and/or renovation to guard facilities.
  - Any other construction or renovation efforts that change or expand the footprint of a facility or structure, including security enhancements to improve perimeter security.
- The following actions and improvements are allowable as non-construction activities under specific HSGP program guidance and must comply with National Environmental Policy Act (NEPA) and other relevant provisions.
  - Improved lighting.
  - Fencing.
  - Closed-circuit television (CCTV) systems.
  - Motion detection systems.
  - Barriers, doors, gates and related security enhancements.
- In addition, the erection of communications towers that are included in a jurisdiction’s interoperable communications plan is allowed, subject to all applicable laws, regulations, and licensing provisions.

***Construction Approval Process for SHSP, UASI, and LETPP***

In order for grantees to drawdown funds for construction and renovation costs under SHSP, UASI, and LETPP, grantees must provide to G&T:

- A description of the asset or facility, asset location, whether the infrastructure is publicly or privately owned, and the construction or renovation project.
- Certification that a facility vulnerability assessment has been conducted for the facility.
- An outline addressing how the construction or renovation project will address the identified vulnerabilities from the assessment.
- Consequences of not implementing the construction or renovation project

Written approval must be provided by G&T prior to the use of any HSGP funds for construction or renovation.

***National Environmental Policy Act (NEPA)***

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

**E. Unallowable Costs Guidance**

Several costs are strictly prohibited under FY 2006 HSGP. Grantees should contact their G&T Preparedness Officer for guidance and clarification.

**E.1. Hiring of Public Safety Personnel**

FY 2006 HSGP funds may not be used to support the hiring of sworn public safety officers for the purposes of fulfilling traditional public safety duties or to supplant traditional public safety positions and responsibilities. See also Appendix D for allowable hiring expenditures.

**E.2. Construction and Renovation**

Construction and renovation is generally prohibited, except as noted above under *Construction and Renovation Guidance* in this Section. Such construction and renovation shall be strictly limited and allowable when it is a necessary component of a security system at critical infrastructure facilities.

**F. Office of Grants and Training Resources and Support**

To assist grantees with program activities, G&T has several support mechanisms available to grantees.

**F.1. Centralized Scheduling and Information Desk (CSID) Help Line**

CSID is a comprehensive coordination, management, information, and scheduling tool developed by 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, and 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.

CSID can be contacted at 1-800-368-6498 or [askcsid@dhs.gov](mailto:askcsid@dhs.gov). CSID hours of operation are from 8:00 a.m. to 7:00 p.m. (EST), Monday through Friday.

## **F.2. Federal Fiscal Support and Oversight**

G&T's Office of Grants Operations (OGO) will provide fiscal support and oversight of the grant programs included in this solicitation. For FY 2006 awards, grant and sub-grant recipients should refer to the OGO Financial Guide. This Guide may be obtained by contacting OGO at 1-866-9ASKOGO or by email at [ask-OGO@dhs.gov](mailto:ask-OGO@dhs.gov). All previous awards are still governed by the OJP Financial Guide, available at <http://www.ojp.usdoj.gov/FinGuide>.

## **F.3. Homeland Security Technical Assistance Programs**

DHS's technical assistance programs seeks to build and sustain State and local jurisdiction capacity related to two primary functional areas: (1) overall homeland security program management; and (2) priority preparedness activities (prevent, protect against, respond to, and recover from major events, including threats or acts of terrorism). This two-pronged approach ensures that technical assistance services measurably contribute to the enhancement of the homeland security architecture within each State and local jurisdiction as well as the associated preparedness capabilities housed therein. The technical assistance services designed, developed, and delivered to State and local homeland security personnel address the spectrum of mission areas, priorities, and capabilities outlined in the interim National Preparedness Goal.

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

## **F.4. Lessons Learned Information Sharing (LLIS) System**

LLIS is a national, online, secure website that houses a collection of peer-validated lessons learned, best practices, and AARs from exercises and actual incidents, and other relevant homeland security documents. LLIS is designed to help emergency response providers and homeland security officials prevent, prepare for, respond to, and recover from major events. LLIS facilitates improved preparedness nationwide by providing response professionals with access to a wealth of validated front-line expertise on effective planning, training, equipping, and operational practices for homeland security.

The LLIS website also includes a national directory of responders and homeland security officials, as well as an updated list of homeland security exercises, events, and conferences. Additionally, LLIS includes online collaboration tools, including secure email and message boards, where users can exchange information. LLIS uses strong encryption and active site



monitoring to protect all information housed on the system. The LLIS website is located at <https://www.llis.gov>.

#### **F.5. Equipment Purchase Assistance Program**

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

#### **F.6. Exercise Direct Support**

DHS has engaged multiple contractors with significant experience in designing, conducting, and evaluating exercises to provide support to States and local jurisdictions in accordance with State Homeland Security Strategies and HSEEP. Contract support is available to help States conduct an Exercise Plan Workshop, develop a Multi-year Exercise Plan and build or enhance the capacity of States and local jurisdictions to design, develop, conduct, and evaluate effective exercises.

Direct support to States and UASI-designated Urban Areas is decided on a priority basis. Priority is given to the conduct of EPWs, preparedness for significant events not designated as National Special Security Events (NSSE), and to meet grant requirements (e.g., Tactical Interoperable Communications Plan requirement). Applications for direct support are available at <http://hseep.dhs.gov> and are reviewed on a monthly basis.

HSEEP offers several tools and resources to help design, develop, conduct and evaluate exercises, including:

- HSEEP Volumes I-IV.
- HSEEP Training (Mobile Course and Independent Study Course).
- HSEEP Toolkit.
- HSEEP Website (<http://hseep.dhs.gov>).

**III. ELIGIBLE  
APPLICANTS AND  
FUNDING AVAILABILITY**

### III. ELIGIBLE APPLICANTS AND FUNDING AVAILABILITY

#### A. Allocating FY 2006 HSGP Funding Based on Risk and Need

The threats confronting the Nation respect neither jurisdictional nor geographic boundaries. Resources must be allocated and applied in an effective and efficient manner to generate the highest return on investment. Following this direction, G&T is adopting a common risk- and needs-based approach to allocating funding for several programs within HSGP in order to strengthen national preparedness. This approach will help ensure that capabilities are built and sustained to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies, while achieving the greatest return on our national investment in homeland security by addressing the greatest risks and needs.

Understanding risk and need, and applying resources effectively to manage them, is critical to national preparedness. Applying the principles of unified command and adopting a systems-based approach to preparedness will enable the development and maintenance of capabilities and programs that will achieve more success in combination with a shared commitment than through individual, disparate efforts. In short, these efforts will help the Nation realize the vision of the Goal.

FY 2006 marks the first grant cycle in which the Interim National Preparedness Goal and the National Priorities it establishes are in place. In keeping with the risk-based focus of the Goal and the President's proposed FY 2006 budget, G&T is adopting a risk- and needs-based approach to allocating funding for three programs within the FY 2006 HSGP: SHSP, LETPP, and UASI.

DHS has elected to provide a base allocation to States under SHSP and LETPP. The remainder of those funds will be allocated based on risk and need. Under UASI, all funding will be allocated based on risk and need. MMRS and CCP will be allocated on a formula basis identical to FY 2005.

##### A.1. Risk and Need

###### *Risk*

Risk will be determined at the Federal level using a risk formula developed by G&T in conjunction with other DHS and Federal entities. The FY 2005 risk analysis used to determine UASI allocations represented the first time DHS grant formulation addressed consequence, vulnerability, and threat. The FY 2006 risk formula builds upon this effort, incorporating suggested improvements and lessons learned. For FY 2006, risk is defined as the product of three principal variables:

- The consequences of a specified attack to a particular asset.
- The vulnerability of that asset to that particular threat.
- Threat to that asset.

The risk formula for the FY 2006 HSGP consists of making two different, but complementary, risk calculations: asset-based risk and geographically-based risk.

- **Asset-based risk** utilizes threat values derived from Intelligence Community assessments of the intent and capability of adversaries to accomplish a set of baseline attack modes. These threats and attack types are mapped against specific infrastructure types (e.g., bridges, dams, and chemical plants).
- **Geographically-based risk** takes into account values that are based on the inherent attributes of the geographical candidate (i.e., State or Urban Area). This analysis takes into account such factors as international borders, terrorism-related reporting and investigations, and population density.

The risk associated with assets is combined with the risk associated with a geographical area to produce a total terrorism risk score.

### *Need*

The needs of State and local governments will be determined as an output of the Program and Capability Review initiative currently underway. This effort seeks to assist States in determining their needs in relation to the capabilities outlined in the Goal through a comprehensive evaluation of their homeland security program and priority capabilities. Through this review process, States will develop two key submissions for the FY 2006 HSGP application:

- *Program and Capability Enhancement Plan*, which is a multi-year global program management plan for the entire State homeland security program that looks beyond G&T grant programs and funding; and
- *Investment Justification*, which identifies areas of specific Initiatives from the Enhancement Plan for which States wish to utilize FY 2006 HSGP funding.

States must use the Investment Justification to outline implementation approaches for specific investments that will go towards achieving the Initiatives outlined in their Enhancement Plan, and justify all funding requested through the HSGP, including all UASI funding, any base allocations for SHSP and LETPP, and all formula allocations under MMRS and CCP.

Applications will be evaluated based on the effectiveness of a State's plan to address priorities it has outlined, and thereby reduce its overall risk. This approach creates incentives for States and Urban Areas to develop innovative solutions and effectively leverage HSGP funds in the management and implementation of their overall homeland security program. Scoring criteria are outlined in the Application Kit section of this document.

Additional information on the Program and Capability Enhancement Plan and Investment Justification, including scoring criteria, are available in Chapter IV Application Kit. Detailed guidance, including an Investment Justification template is available in Appendix B.

All Investment Justifications will be formally reviewed and scored through a peer review process. States will be notified of their final total allocation at the time of award.

## B. Eligible Applicants

The FY 2006 HSGP integrates SHSP, UASI, LETPP, MMRS, and CCP into a single application kit. Funding from this combined program will significantly enhance the ability of States, Urban Areas, and local agencies to prevent, protect, respond to, and recover from threats and incidents of terrorism. The Governor of each State has designated a State Administrative Agency (SAA) to apply for and administer the funds under HSGP.<sup>11</sup> The SAA is the only agency eligible to apply for HSGP funds and is responsible for obligating HSGP funds to local units of government and other designated recipients.<sup>12</sup>

## C. Funding

### C.1. FY 2006 SHSP and LETPP Allocations

Each State will receive a base allocation under SHSP and LETPP using the USA PATRIOT Act formula. Accordingly, all 50 States, the District of Columbia, and Puerto Rico will receive 0.75 percent of the total allocation for those programs. Four Territories (American Samoa, Guam, Northern Mariana Islands, and the Virgin Islands) will receive a base allocation 0.25 percent of the total for SHSP and LETPP. The remainder of funds will be allocated based on an analysis of risk and need mentioned above.

### C.2. FY 2006 UASI Allocations

FY 2006 UASI funds will be allocated based on risk and need upon completion of the application review process. Eligible applicants for UASI allocations are still under consideration. DHS will release the list of UASI candidates shortly after this release of the FY 2006 HSGP guidance.

### C.3. FY 2006 MMRS Jurisdictions

FY 2006 MMRS funding will be divided evenly among the current 124 MMRS jurisdictions listed in Table 6.

**Table 6 – MMRS Jurisdictions**

State	MMRS Jurisdictions
Alabama	Birmingham, Huntsville, Mobile, and Montgomery
Alaska	Anchorage and Southeast Alaska
Arizona	Glendale, Mesa, Phoenix, and Tucson
Arkansas	Little Rock

<sup>11</sup> As defined in the Homeland Security Act of 2002, the term “State” means “any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States”

<sup>12</sup> As defined in the Conference Report accompanying the Department of Homeland Security Appropriations Act of 2006, the term “local unit of government” means “any county, city, village, town, district, borough, parish, port authority, transit authority, intercity rail provider, commuter rail system, freight rail provider, water district, regional planning commission, council of government, Indian tribe with jurisdiction over Indian country, authorized Tribal organization, Alaska Native village, independent authority, special district, or other political subdivision of any State.”

State	MMRS Jurisdictions
California	Los Angeles, San Francisco, San Diego, San Jose, Long Beach, Oakland, Sacramento, Fresno, Santa Ana, Anaheim, Riverside, Glendale, Huntington Beach, Stockton, Bakersfield, Fremont, Modesto, and San Bernardino
Colorado	Aurora, Colorado Springs, and Denver
Connecticut	Hartford
Florida	Miami, Jacksonville, Tampa, St. Petersburg, Hialeah, Ft. Lauderdale, and Orlando
Georgia	Atlanta and Columbus
Hawaii	Honolulu
Illinois	Chicago
Indiana	Ft. Wayne and Indianapolis
Iowa	Des Moines
Kansas	Kansas City and Wichita
Kentucky	Lexington/Fayette and Louisville
Louisiana	Baton Rouge, Jefferson Parish, New Orleans, and Shreveport
Maryland	Baltimore
Massachusetts	Boston, Springfield, and Worcester
Michigan	Detroit, Grand Rapids, and Warren
Minnesota	Minneapolis and St. Paul
Mississippi	Jackson
Missouri	Kansas City and St. Louis
Nebraska	Lincoln and Omaha
Nevada	Las Vegas
New Hampshire	Northern New England MMRS (also serves Maine and Vermont)
New Jersey	Jersey City and Newark
New Mexico	Albuquerque
New York	Buffalo, New York City, Rochester, Syracuse, and Yonkers
North Carolina	Charlotte, Greensboro, and Raleigh
Ohio	Akron, Cincinnati, Cleveland, Columbus, Dayton, and Toledo
Oklahoma	Oklahoma City and Tulsa
Oregon	Portland
Pennsylvania	Allegheny County and Philadelphia
Rhode Island	Providence
South Carolina	Columbia
Tennessee	Chattanooga, Knoxville, Memphis, and Nashville
Texas	Amarillo, Arlington, Austin, Corpus Christi, Dallas, El Paso, Fort Worth, Garland, Houston, Irving, Lubbock, San Antonio, and Southern Rio Grande
Utah	Salt Lake City
Virginia	Arlington County, Chesapeake, Newport News, Norfolk, Richmond, and Virginia Beach
Washington	Seattle, Spokane, and Tacoma
Wisconsin	Madison and Milwaukee
<b>TOTAL</b>	<b>124 MMRS Jurisdictions</b>

**C.4. FY 2006 CCP Allocations**

CCP allocations are determined using a base amount of 0.75 percent of the total allocation for each State (including the District of Columbia and the Commonwealth of Puerto Rico), and 0.25 percent of the total allocation for each U.S. Territory. The balance of funds for CCP is distributed on a population-share basis.

## **IV. APPLICATION KIT**

## IV. APPLICATION KIT

SAAAs must apply for FY 2006 HSGP funding through the online Grants Management System (GMS) at <https://grants.ojp.usdoj.gov/>. Applications must be received by G&T no later than ***Thursday, March 2, 2006***. G&T will evaluate and act on applications within 90 days of the application deadline. A portion of SHSP, UASI, and LETPP funds will be awarded based on risk and need through a quasi-competitive process. States should also be aware of the possibility that due to this quasi-competitive process, they may not receive all of the funding which they request. As such, it is absolutely critical that States submit complete applications no later than March 2, 2006. Award totals may be negatively impacted should applications be submitted after the deadline. States will be informed of funding decisions after G&T evaluates and acts on applications.

The program title listed in the Catalog of Federal Domestic Assistance (CFDA) at <http://12.46.245.173/cfda/cfda.html> is “Homeland Security Grant Program.” The CFDA number for FY 2006 HSGP is 97.067. When completing the online application, applicants should identify their submissions as new, non-construction applications. The project period will be for a period not to exceed 24 months. Table 7 outlines the required application elements.

**Table 7 – Application Checklist**

<p style="text-align: center;"><b>Applicants must complete the following for the FY 2006 HSGP application:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <b>SF-424 Grant Application with Certifications (through GMS)</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Non-Supplanting Certification</li> <li><input type="checkbox"/> Assurances</li> <li><input type="checkbox"/> Certifications Regarding Lobbying; Debarment, Suspension, and Other Responsibility Matters; and Drug-Free Workplace Requirement</li> </ul> </li> <li><input type="checkbox"/> <b>DUNS Number</b></li> <li><input type="checkbox"/> <b>For Urban Areas (if applicable):</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> State, Core City(ies), and Core County(ies) POCs</li> <li><input type="checkbox"/> Urban Area Definition</li> <li><input type="checkbox"/> Establish UAWG, including structure and membership</li> </ul> </li> <li><input type="checkbox"/> <b>Review of Application by the State Single Point of Contact (SPOC)</b></li> <li><input type="checkbox"/> <b>Program and Capability Enhancement Plan</b></li> <li><input type="checkbox"/> <b>Investment Justification</b></li> </ul> <p><b>Grantees must also submit the following to receive funding:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <b>NIMS FY05 Certification Form (Deadline: September 30, 2005)</b></li> <li><input type="checkbox"/> <b>Review of State Emergency Operations Plans (Deadline: January 17, 2006)</b></li> </ul>
--

### Required FY 2006 HSGP Application Submissions

#### 1. SF-424 Grant Application with Certifications (through GMS)

- **Non-Supplanting Certification:** This certification from the SAA, which is a required component of the online GMS application, affirms that Federal funds will only be used to supplement existing funds and will not replace (supplant) funds that have been appropriated for the same purpose. Potential supplanting will be addressed in the



application review as well as in the pre-award review, post-award monitoring, and audit. Applicants or grantees may be required to supply documentation certifying that a reduction in non-Federal resources occurred for reasons other than the receipt or expected receipt of Federal funds.

- **Match Requirement:** There is no match requirement.
  - **Assurances:** The online GMS application includes a list of assurances that the applicant must comply with in order to receive Federal funds under this program. It is the responsibility of the recipient of the Federal funds to fully understand and comply with these requirements. Failure to comply may result in the withholding of funds, termination of the award, or other sanctions. The applicant agrees to these assurances upon the submission of the application.
  - **Certifications Regarding Lobbying; Debarment, Suspension, and Other Responsibility Matters; and Drug-Free Workplace Requirement:** This certification, which is a required component of the online application, commits the applicant to compliance with the certification requirements under 28 Code of Federal Regulations (CFR) part 67, *Government-wide Debarment and Suspension (Non-procurement)*; 6 CFR part 9, *New Restrictions on Lobbying*, and 28 CFR part 83 *Government-wide Requirements for Drug-Free Workplace (Grants)*. All of these regulations can be referenced at <http://www.gpoaccess.gov/cfr/index.html>. The certification will be treated as a material representation of the fact upon which reliance will be placed by DHS in awarding grants.
  - **Suspension or Termination of Funding:** DHS, by written notice, may terminate this grant, in whole or in part, when it is in the Government's interest.
2. **DUNS Number.** The SAA must provide a Dun and Bradstreet (D&B) Data Universal Numbering System (DUNS) number with the FY 2006 HSGP application. An application will not be considered complete until a valid DUNS number is provided by the applicant. This number may be provided in one of the attachment fields within the online GMS application. Organizations should verify that they have a DUNS number or take the steps necessary to obtain one as soon as possible. Applicants can receive a DUNS number at no cost by calling the dedicated toll-free DUNS Number request line at 1-800-333-0505.
3. **For identified UASI Urban Areas:**
- **Identify Points of Contact:** For new Urban Areas, the SAA must designate a specific point of contact (POC) to work with G&T and the designated Urban Area on implementation of the FY 2006 UASI. The SAA POCs are then responsible for identifying and coordinating with a POC from the Urban Area Working Group. This information must be provided to G&T along with the grant application. Existing Urban Areas must ensure that information for current POCs is on file with G&T.

- Define the Urban Area:** For new Urban Areas, the SAA POC, in coordination with the candidate Urban Areas, as outlined in Chapter VII, UASI Program Guidance, must fully define the Urban Area, as it will apply to FY 2006 UASI. The identified city or combined entity represents the candidate Urban Area eligible to apply for funding under the FY 2006 UASI program. For those Urban Areas with a combined entity, that area represents the minimum area that must be part of the defined Urban Area. The definition of the Urban Area is limited to jurisdictions contiguous to the geographic area used to determine eligibility, or with which jurisdictions in that area have established formal mutual aid agreements. States may request a waiver for this limitation for regions previously established by Executive Order, law or compact. For the purposes of the FY 2006 UASI, the Washington, D.C. Urban Area will consist of the National Capital Region (NCR) as set forth in 10 U.S.C. 2674(f)(2).

In coordination with the Urban Area Working Group (UAWG), the SAA POC may redefine the geographic boundaries of an existing Urban Area, as it will apply to the FY 2006 UASI Program. The SAA POC must notify G&T of this change.

- Establish the Urban Area Working Group (UAWG):** Membership in the UAWG must provide either direct or indirect representation for all the jurisdictions that comprise the defined Urban Area. The SAA POC, in coordination with the eligible Urban Area, must determine appropriate representation for that geographic area to serve on the UAWG. Furthermore, where there is a Regional Transit Security Working Group (RTSWG) or a Area Maritime Security Committee active within the geographical area, the UAWG should include them as functional sub-committees to their organization. G&T strongly encourages that, wherever possible, previously established local working groups be leveraged for this purpose. Local MMRS and Citizen Corps Council representatives must be included as well. An overview of the UAWG structure and a list of members and their associated jurisdictions must be provided to G&T along with the grant application. New Urban Areas must provide to G&T an overview of the UAWG structure, a list of members, and their associated jurisdictions along with the grant application. Existing Urban Areas must notify G&T of any updates to the UAWG structure or membership.

- 4. Single Point of Contact (SPOC) Review:** Executive Order 12372, located at <http://www.archives.gov/federal-register/codification/executive-order/12372.html> requires applicants from State and local units of government or other organizations providing services within a State to submit a copy of the application to the State SPOC, if one exists, and if this program has been selected for review by the State. Applicants must contact their State SPOC to determine if the program has been selected for State review. The date that the application was sent to the SPOC or the reason such submission is not required should be provided.
- 5. Program and Capability Enhancement Plan:** On October 31, 2005, G&T released preliminary guidance on conducting a Program and Capability Review and developing a Program and Capability Enhancement Plan. The Enhancement Plan is the key building block in the process States will use to develop an Investment Justification for FY 2006 HSGP funds. States should use the template disseminated on November 14, 2005, in the *State*

*Homeland Security Program and Capability Review Guidebook Volume II: Enhancement Plan* to develop their Enhancement Plans. The Enhancement Plan frames the resource needs required to build and sustain the capabilities analyzed in the Program and Capability Review. The Enhancement Plan is intended to serve as an enterprise-wide program management plan for the State homeland security program. It is not linked to or associated with one particular grant program or funding stream. Rather, it is intended to look globally at the prioritized needs of the State homeland security program across all Urban Areas, jurisdictions, and disciplines.

- 6. Investment Justification:** States will use the Program and Capability Enhancement Plan to identify areas from their Enhancement Plan for which they wish to utilize FY 2006 HSGP funding. States will develop an Investment Justification to request FY 2006 HSGP funds for those areas from the Enhancement Plan they have identified as priorities to use FY 2006 HSGP funding in the near-term. An Investment Justification template will be provided to the States to facilitate the application submission process. In the Investment Justification template, States will outline which Initiatives identified in their Enhancement Plans they wish to support in whole or in part through FY 2006 HSGP funding.

The Investment Justification template includes blank worksheets for States and Urban Areas to complete that are divided into the following four sections:

- Background.
- Regionalization.
- Impact.
- Funding and Implementation Plan.

States and Urban Areas must submit an individual worksheet within the Investment Justification template for each investment they are requesting FY 2006 SHSP, UASI, LETPP, MMRS, and CCP funding. The template also includes a summary sheet that is populated automatically with information from the individual investment worksheets.

A maximum of 15 investments may be submitted per State. Additionally, Urban Areas will also be allowed to propose up to 15 investments to request UASI funds, separate from the 15 State investments. While States and Urban Areas will develop their own investments, **the Urban Area investments must be included as part of the overall State application.** States and Urban Areas are strongly encouraged to coordinate with each other to present an application that represents a collaborative, integrated approach, and to avoid duplication of efforts. The sum of the investments must account for all FY 2006 HSGP funding the States and Urban Areas are requesting across all programs.

The Investment Justification will be used to review applications for completeness, adherence to programmatic guidelines, feasibility, and how well the proposed solution addresses the need identified in the Enhancement Plan. The Investment Justification will also be used to score applications and make funding decisions for the needs-based component of HSGP. Evaluation points will include:

- Relevance to the Goal, National Priorities, Target Capabilities, State/Urban Area Homeland Security Strategy goals and objectives, and Enhancement Plan Initiatives.
- Regionalization and effective collaboration.
- Sustainability.
- Implementation Approach.
- Impact.

States and Urban Areas are required to use the Investment Justification template developed in Microsoft® Excel. The template and user instructions will be disseminated under separate correspondence. Character limitations will be enforced for narrative responses in the Investment Justification template, and are noted in the instructions where applicable. The SAA must upload the State and appropriate Urban Area(s) Investment Justifications as attachments in GMS when submitting the FY 2006 HSGP application. Additional information on the Investment Justification is included in Appendix B.

**Applicants must familiarize themselves with the requirements and restrictions of the Program Guidance for FY 2006 HSGP, available in Section II of this document. All grant recipients are assumed to have read, understood, and accepted the Program Guidance as binding.**

# **V. AWARD AND REPORTING REQUIREMENTS**

## V. AWARD AND REPORTING REQUIREMENTS

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

- Percent of jurisdictions demonstrating acceptable performance on applicable critical tasks in exercises using approved scenarios.
- Percent of State and local homeland security agency grant recipients reporting measurable progress towards identified goals and objectives to prevent and respond to terrorist attacks.
- Percent progress toward implementation of State strategies observed by Preparedness Officers.
- Percent of participating Urban Area grant recipients reporting measurable progress made towards identified goals and objectives to prevent and respond to terrorist attacks.
- Percent progress toward State strategies implementation for Urban Area Grant Recipients observed by preparedness officers.

To collect and report on these measures, the Department will use information from: after-action reports (AARs) from homeland security exercises using the Homeland Security Exercise and Evaluation Program (HSEEP) doctrine and general information from State Strategies, Bi-Annual Strategy Implementation Reports, and Grant Monitoring Reports. Please note that the Department does not use this general performance information as a basis for awarding State and local grants; rather, the Department uses the information to assess overall program effectiveness and impact and to report results to Congress, the Office of Management and Budget, and the President.

### A. Grant Award and Obligation of Funds

Upon approval of the application, the grant will be awarded to the respective SAA. This date will be known as the “award date.” The signed award document with special conditions must be returned to OGO. See Appendix A for additional information. The State’s obligation period must be met within **60 days** of the award date. An obligation is defined as a definite commitment which creates a legal liability for the payment of funds for goods and services ordered or received. Four requirements must be met to obligate grant funds:

- There must be some action to establish a firm commitment on the part of the awarding entity.
- The condition must be unconditional on the part of the awarding entity.
- There must be documentary evidence of the commitment.
- The award terms must be communicated to the official grantee.

Within 60 days of the grant award, the SAA will submit a prioritization of investments based upon the final grant award amounts and a certification that funds have been passed through to local units of government (to include the identification of subgrantees and sub-award amounts.)

## **B. Drawdown of Funds**

Following the acceptance of the grant award and the release of any special conditions withholding funds, the grantee can drawdown funds through the following methods: the Automated Standard Application for Payments (ASAP), Phone Activated Paperless Response System (PAPRS), or Letter Of Credit Electronic Certification System (LOCES).

In support of continuing efforts 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 (5) working days of each month. SAAs should make payment requests before the last five working days of the month to avoid delays in deposit of payments. For example, for the month of September, the last day to request (drawdown) payments was September 23, 2005. Payments requested after September 23, 2005, will be processed when the regular schedule resumed on October 1, 2005. A similar schedule will follow at the end of each month thereafter.

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

Questions regarding grant payments should be addressed to the OJP OC at 1-800-458-0786 or email [askoc@ojp.usdoj.gov](mailto: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](mailto:ask-ogo@dhs.gov).

## **C. Reporting Requirements**

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

### **C.1 Financial Status Report (FSR) (Required quarterly)**

Obligations and expenditures must be reported to G&T on a quarterly basis through the FSR, which is due within 30 days of the end of each calendar quarter (e.g., for the quarter ending March 31, FSR is due on April 30). Please note that this is a change from previous fiscal years. A report must be submitted for every quarter the award is active, including partial calendar quarters, as well as for periods where no grant activity occurs. A copy of this form will be included in the initial award package. Also, FSRs may be filed on-line through the internet at <http://grants.ojp.usdoj.gov>. Future awards and fund drawdowns will be withheld if these reports are delinquent.

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

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

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

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

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

The BSIR and the CAPR are due within 30 days after the end of the reporting period (July 31 with a reporting period of January 1 through June 30, and on January 31 with a reporting period of July 1 through December 31). Updated obligation and expenditure information must be provided with the BSIR to show progress made toward meeting strategic goals and objectives. G&T will provide a web-enabled application for the BSIR submission to grantees and a copy of the CAPR (OJP Form 4587/1) in the initial award package. Future awards and fund drawdowns may be withheld if these reports are delinquent. The final BSIR is due 90 days after the end date of the award period.

## **C.3 Exercise Evaluation and Improvement**

Exercises implemented with grant funds should be threat- and performance-based and should evaluate performance of critical tasks required to respond to the exercise scenario. Guidance on conducting exercise evaluations and implementing improvement is defined in the HSEEP Volume: *Exercise Evaluation and Improvement* located at <http://hseep.dhs.gov>. Exercises must be included in the Multiyear Exercise Plan calendar, and added to the National Exercise



Schedule through the G&T Secure Portal. The SAA must report on scheduled exercises and ensure that an 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 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 the HSEEP manuals.

#### **C.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 HSGP assistance for audit and examination purposes, provided that, in the opinion of the Secretary of Homeland Security or the Comptroller General, these documents are related to the receipt or use of such assistance. The grantee will also give the sponsoring agency or the Comptroller General, through any authorized representative, access to, and the right to, examine all records, books, papers or documents related to the grant.

The State shall require that subgrantees comply with the audit requirements set forth in *OMB Circular A-133*. Recipients are responsible for ensuring that sub-recipient audit reports are received and for resolving any audit findings.

#### **D. Monitoring**

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

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

maintaining of adequate financial records, and the refunding of expenditures disallowed by audits.

### **E. Grant Close-Out Process**

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

# **VI. STATE HOMELAND SECURITY PROGRAM**

## VI. STATE HOMELAND SECURITY PROGRAM

### A. Program Overview

SHSP is a core homeland security assistance program that provides funds to build capabilities at the State and local levels through planning, equipment, training, and exercise activities and to implement the goals and objectives included in Homeland Security Strategies. SHSP funding also supports the four mission areas of homeland security—prevent, protect, respond, and recover—and addresses all of the National Priorities and the 37 Target Capabilities, as they relate to terrorism.

FY 2006 SHSP funding remains primarily focused on enhancing capabilities to prevent, protect against, respond to, or recover from CBRNE, agriculture, and cyber terrorism incidents. However, in light of several major new national planning priorities, which address such issues as pandemic influenza and the aftermath of Hurricane Katrina, the allowable scope of SHSP activities include catastrophic events, provided that these activities also build capabilities that relate to terrorism.

Many of the capabilities included within the TCL are dual-use in nature, in that they can apply to both terrorism preparedness as well as other hazards. Activities implemented under SHSP must support terrorism preparedness and build or enhance capabilities that relate to terrorism in order to be considered eligible, even if the capabilities themselves do not focus exclusively on terrorism. For example, mass evacuation planning supports terrorism preparedness but also other types of catastrophic events. Planning for pandemic influenza and linking that effort to a larger bioterrorism preparedness effort offers another example. Grantees must demonstrate the dual-use nature of any activities implemented under this program that are not explicitly focused on terrorism preparedness.

As defined in the Catastrophic Incident Supplement to the NRP, a catastrophic incident is any natural, technical, or manmade incident, including terrorism, that results in extraordinary levels of mass casualties, damage, or destruction severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. A catastrophic event could

#### Target Capabilities

- Planning
- Community Preparedness and Participation
- Communications
- Risk Management
- Info Gathering & Recognition of Indicators & Warnings
- Law Enforcement Investigation and Operations
- Intelligence Analysis & Production
- CBRNE Detection
- Intelligence/Information Sharing & Dissemination
- Critical Infrastructure Protection
- Epidemiological Surveillance & Investigation
- Public Health Laboratory Testing
- Food & Ag. Safety & Defense
- On-Site Incident Management
- Citizen Protection: Evacuation and/or In-Place Protection
- Emergency Operations Center Management
- Isolation & Quarantine
- Critical Resource Logistics & Distribution
- Urban Search & Rescue
- Volunteer Management & Donations
- Emergency Public Info & Warning
- Responder Safety & Health
- Triage & Pre-Hospital Treatment
- Public Safety & Security Response
- Medical Surge
- Animal Health Emergency Support
- Medical Supplies Management & Distribution
- Environmental Health
- Mass Prophylaxis
- Explosive Device Response Operations
- Mass Care
- Firefighting Operations/Support
- Fatality Management
- WMD/HazMat Response & Decon
- Structural Damage Assessment & Mitigation
- Economic & Community Recovery
- Restoration of Lifelines

result in sustained national impacts over a prolonged period of time; almost immediately exceeds resources normally available to State, local, Tribal, and private sector authorities in the impacted area; and significantly interrupts governmental operations and emergency services to such an extent that national security could be threatened. Catastrophic events result in unique challenges regarding such issues as mass care, search and rescue, victim and fatality management and transportation, public health and medical support, and public information, many of which are also critical issues for terrorism preparedness.

Grantees may use SHSP funding to achieve or enhance all of the 37 capabilities, as long as they enhance the capability to prevent, protect against, respond to, or recover from acts of terrorism. Grantees should consult the Catastrophic Incident Supplement to the NRP and the planning assumptions upon which it is centered to understand the scope of catastrophic incidents relative to their own prioritization of capabilities and resource allocations. Grantees should focus their proposed FY 2006 Investments on the National Priorities and their most urgent State/local priorities.

The Goal identifies enhanced regional collaboration as a national priority. States must employ regional approaches to planning and preparedness and are encouraged to adopt regional response structures whenever appropriate to meet the needs identified through assessments and in the Homeland Security Strategies.

## **B. Program Requirements**

Use of SHSP funds must be consistent with and supportive of implementation of the State Homeland Security Strategy. Linkages between specific projects undertaken with SHSP funds and strategic goals and objectives will be highlighted through regular required reporting mechanisms, including the BSIR.

## **C. Authorized Program Expenditures**

This section provides guidance on the types of expenditures that are allowable under the SHSP. Please refer to the checklist in Appendix D for a summary of authorized and unauthorized SHSP expenditures.

### **C.1. Planning**

FY 2006 SHSP funds may be used for a range of homeland security planning activities, such as:

- Developing and implementing homeland security support programs and adopting DHS national initiatives including but not limited to the following:
  - o Implementing the National Preparedness Goal and Guidance.
  - o Implementing and adopting NIMS.
  - o Modifying existing incident management and Emergency Operating Procedures (EOPs) to ensure proper alignment with the NRP coordinating structures, processes, and protocols.

- o Establishing or enhancing mutual aid agreements.
- o Developing communications and interoperability protocols and solutions.
- o Conducting local, regional, and Tribal program implementation meetings.
- o Developing or updating resource inventory assets in accordance to typed resource definitions issued by the NIMS Integration Center (NIC).
- o Designing State and local geospatial data systems.
- o Conducting public education and outreach campaigns, including promoting individual, family and business emergency preparedness; alerts and warnings education; and evacuation plans.
- Developing related terrorism prevention activities including:
  - o Planning to enhance security during heightened alerts, during terrorist incidents, and/or during mitigation and recovery.
  - o Multi-discipline preparation across first responder community, including EMS for response to catastrophic events and acts of terrorism.
  - o Public information/education: printed and electronic materials, public service announcements, seminars/town hall meetings, web postings coordinated through local Citizen Corps Councils.
  - o Citizen Corps volunteer programs and other activities to strengthen citizen participation.
  - o Conducting public education campaigns, including promoting individual, family and business emergency preparedness; promoting the *Ready* campaign; and/or creating State, regional or local emergency preparedness efforts that build upon the *Ready* campaign.
  - o Evaluating CIP security equipment and/or personnel requirements to protect and secure sites.
  - o CIP cost assessments, including resources (e.g., financial, personnel) required for security enhancements/deployments.
- Developing and enhancing plans and protocols, including but not limited to:
  - o Developing or enhancing EOPs and operating procedures.
  - o Developing terrorism prevention/deterrence plans.
  - o Developing plans, procedures, and requirements for the management of infrastructure and resources related to HSGP and implementation of State or Urban Area Homeland Security Strategies.
  - o Developing or enhancing border security plans.
  - o Developing or enhancing cyber security plans.
  - o Developing or enhancing cyber risk mitigation plans.
  - o Developing or enhancing agriculture/food security risk mitigation, response, and recovery plans.
  - o Developing public/private sector partnership emergency response, assessment, and resource sharing plans.
  - o Developing or updating local or regional communications plans.
  - o Developing plans to support and assist special needs jurisdictions, such as port authorities and rail and mass transit agencies.
  - o Developing or enhancing continuity of operations and continuity of government plans.

- o Developing or enhancing existing catastrophic incident response and recovery plans to include and integrate Federal assets provided under the NRP.
- o Developing or enhancing evacuation plans.
- o Developing or enhancing citizen surge capacity.
- Developing or conducting assessments, including but not limited to:
  - o Conducting point vulnerability assessments at critical infrastructure sites/key assets and develop remediation/security plans.
  - o Conducting cyber risk and vulnerability assessments.
  - o Conducting assessments and exercising existing catastrophic incident response and recovery plans and capabilities to identify critical gaps that cannot be met by existing local and State resources.
  - o Activities that directly support the identification of specific catastrophic incident priority response and recovery projected needs across disciplines (e.g. law enforcement, fire, EMS, public health, behavioral health, public works, agriculture, information technology, and citizen preparedness).
  - o Activities that directly support the identification of pre-designated temporary housing sites.

## **C.2. Organization**

Organization costs are not allowed under SHSP.

## **C.3. Equipment**

FY 2006 SHSP funds may be used for equipment acquisition from the 21 equipment categories listed in the FY 2006 G&T AEL. The FY 2006 AEL is available in its entirety online through the RKB at <http://www.rkb.mipt.org> and the equipment categories are outlined in Table 8 below and Appendix D.

**Table 8 – SHSP Allowable Equipment Categories**

#	Category Title	#	Category Title
[1]	Personal Protective Equipment	[12]	CBRNE Incident Response Vehicles
[2]	Explosive Device Mitigation and Remediation Equipment	[13]	Terrorism Incident Prevention Equipment
[3]	CBRNE Operational and Search and Rescue Equipment	[14]	Physical Security Enhancement Equipment
[4]	Information Technology	[15]	Inspection and Screening Systems
[5]	Cyber Security Enhancement Equipment	[16]	Agricultural Terrorism Prevention, Response and Mitigation Equipment
[6]	Interoperable Communications Equipment	[17]	CBRNE Prevention and Response Watercraft
[7]	Detection Equipment	[18]	CBRNE Aviation Equipment
[8]	Decontamination Equipment	[19]	CBRNE Logistical Support Equipment
[9]	Medical Supplies and Limited Types of Pharmaceuticals	[20]	Intervention Equipment
[10]	Power Equipment	[21]	Other Authorized Equipment
[11]	CBRNE Reference Materials		

**C.4. Training**

FY 2006 SHSP funds may be used to enhance the capabilities of State and local emergency preparedness and response personnel through development of a State homeland security training program. Allowable training-related costs include:

1. Establishment of support for, conduct of, and attendance at preparedness training programs within existing training academies/institutions, universities, or junior colleges. Preparedness training programs are defined as those programs related to prevention, protection, response, and or recovery from natural, technical, or manmade catastrophic incidents, supporting one or more Target Capabilities in alignment with national priorities as stated in the Goal. Examples of such programs include but are not limited to CBRNE terrorism, critical infrastructure protection, cyber security, and citizen preparedness.
2. Overtime and backfill costs associated with attendance at G&T-sponsored and approved training courses. SHSP may also be used for training citizens in awareness, prevention, protection, response, recovery skills

**C.5. Exercises**

SHSP funds may be used to design, develop, conduct, and evaluate exercises that:

- Provide homeland security preparedness personnel and volunteers a venue to practice prevention, protection, response, and recovery activities.
- Evaluate prevention and response plans, policy, procedures, and protocols, including NIMS and NRP.
- Assess the readiness of jurisdictions to prevent and respond to terrorist attacks.
- Encourage coordination with surrounding jurisdictions in prevention, protection, response, and recovery activities.



**C.6. Personnel**

Hiring, overtime, and backfill expenses are allowable only to perform programmatic activities deemed allowable under existing guidance. Supplanting, however, is not allowed.

Up to 15% of programmatic spending may be used to support the hiring of full or part-time personnel to conduct program activities that are allowable under the entire FY 2006 HSGP (i.e., planning, training program management, exercise program management, etc). Grantees may request that DHS issue a waiver to increase that ceiling. Waiver decisions are at the discretion of DHS and will be considered on a case-by-case basis. The ceiling on personnel costs does not apply to contractors, and is in addition to eligible M&A costs and eligible hiring of intelligence analysts. Grantees may hire staff only for program management functions not operational duties. Hiring planners, training program coordinators, exercise managers, and grant administrators fall within the scope of allowable program management functions. Grant funds may not be used to support the hiring of sworn public safety officers to fulfill traditional public safety duties.

**C.7. Management and Administration**

No more than 5 percent of the State's allocation under SHSP may be used for M&A. Local jurisdiction subgrantees may retain and use up to 3 percent of their subaward from the State for local M&A purposes. States may pass through a portion of the State M&A allocation to local subgrantees in order to supplement the 3 percent M&A allocation allowed on subgrants. However, no more than 5 percent of the total subaward may be expended by subgrantees on M&A costs.

# **VII. URBAN AREAS SECURITY INITIATIVE**

## VII. URBAN AREAS SECURITY INITIATIVE

### A. Program Overview

The FY 2006 UASI program provides financial assistance to address the unique multi-discipline planning, operations, equipment, training, and exercise needs of high-threat, high-density Urban Areas, and to assist them in building and sustaining capabilities to prevent, protect against, respond to, and recover from threats or acts of terrorism. FY 2006 UASI funding remains primarily focused on enhancing capabilities to prevent, protect against, respond to, or recover from CBRNE, agriculture, and cyber terrorism incidents. However, in light of several major new national planning priorities, which address such issues as pandemic influenza and the aftermath of Hurricane Katrina, the allowable scope of UASI activities including catastrophic events, provided that these activities also build capabilities that relate to terrorism.

Many of the capabilities included within the TCL are dual-use in nature, in that they can apply to both terrorism preparedness as well as other hazards. Activities implemented under UASI must support terrorism preparedness and build or enhance capabilities that relate to terrorism in order to be considered eligible, even if the capabilities themselves do not focus exclusively on terrorism. For example, mass evacuation planning supports terrorism preparedness but also other types of catastrophic events. Planning for pandemic influenza and linking that effort to a larger bioterrorism preparedness effort offers another example. Grantees must demonstrate the dual-use nature of any activities implemented under this program that are not explicitly focused on terrorism preparedness.

As defined in the Catastrophic Incident Supplement to the NRP, a catastrophic incident is any natural, technical, or manmade incident, including terrorism, that results in extraordinary levels of mass casualties, damage, or destruction severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. A catastrophic event could result in sustained national impacts over a prolonged period of time; almost immediately exceeds resources normally available to State, local, Tribal, and private sector authorities in the impacted area; and significantly interrupts governmental operations

#### Target Capabilities

- Planning
- Community Preparedness and Participation
- Communications
- Risk Management
- Info Gathering & Recognition of Indicators & Warnings
- Law Enforcement Investigation and Operations
- Intelligence Analysis & Production
- CBRNE Detection
- Intelligence/Information Sharing & Dissemination
- Critical Infrastructure Protection
- Epidemiological Surveillance & Investigation
- Public Health Laboratory Testing
- Food & Ag. Safety & Defense
- On-Site Incident Management
- Citizen Protection: Evacuation and/or In-Place Protection
- Emergency Operations Center Management
- Isolation & Quarantine
- Critical Resource Logistics & Distribution
- Urban Search & Rescue
- Volunteer Management & Donations
- Emergency Public Info & Warning
- Responder Safety & Health
- Triage & Pre-Hospital Treatment
- Public Safety & Security Response
- Medical Surge
- Animal Health Emergency Support
- Medical Supplies Management & Distribution
- Environmental Health
- Mass Prophylaxis
- Explosive Device Response Operations
- Mass Care
- Firefighting Operations/Support
- Fatality Management
- WMD/HazMat Response & Decon
- Structural Damage Assessment & Mitigation
- Economic & Community Recovery
- Restoration of Lifelines

and emergency services to such an extent that national security could be threatened. Catastrophic events result in unique challenges regarding such issues as mass care, search and rescue, victim and fatality management and transportation, public health and medical support, and public information, many of which are also critical issues for terrorism preparedness.

Grantees may use UASI funding to achieve or enhance all of the 37 capabilities, as long as they enhance the capability to prevent, protect against, respond to, or recover from acts of terrorism. Grantees should consult the Catastrophic Incident Supplement to the NRP and the planning assumptions upon which it is centered to understand the scope of catastrophic incidents relative to their own prioritization of capabilities and resource allocations. Grantees should focus their proposed FY 2006 Investments on the National Priorities and their most urgent State/local priorities.

The FY 2006 UASI program further provides the opportunity to enhance regional preparedness efforts. Urban Areas must employ regional approaches to overall preparedness and are encouraged to adopt regional response structures whenever appropriate to meet the goals identified in the Urban Area Homeland Security Strategy. Furthermore, it is G&T's intent to guide State and Urban Area security and preparedness efforts toward a process to address common, measurable objectives. Security and preparedness officials at all levels should seek opportunities to leverage funding from multiple sources whenever possible and not restrict their activities to Federal funding alone. This funding will be provided to identified Urban Area authorities through the SAAs. In some instances Urban Area boundaries cross State borders. States must ensure that the identified Urban Areas take an inclusive regional approach to the development and implementation of the FY 2006 UASI program and involve the contiguous jurisdictions, mutual aid partners, port authorities, rail and transit authorities, State agencies, Citizen Corps Council(s), and MMRS(s) in their program activities.

G&T encourages all current and former geographically contiguous Urban Areas to continue existing coordinated and collaborative planning structures and efforts in developing, integrating, and implementing homeland security activities. This includes, but is not limited to, participation on advisory committees and working groups involved in homeland security planning and preparedness processes and activities.

## **B. Program Requirements**

The State agency with overall responsibility for developing the State Homeland Security Strategy and administering G&T programs will be responsible for the administration of the FY 2006 UASI program.

**Data Count for FY 2006 UASI Eligibility Determination:** To identify jurisdictions for inclusion in the data count phase, all cities with a population greater than 100,000 and any city with reported threat data during the past year were identified. Cities on this list with shared city boundaries were combined into a single entity for data count purposes. A 10-mile buffer was then drawn from the border of that city or combined entity to establish the geographical area in which data was evaluated.

**Governance:** The identified city or combined entity represents the candidate Urban Area eligible to apply for funding under the FY 2006 UASI program. For those Urban Areas with a combined entity, that area represents the minimum area that must be part of the defined Urban Area. States and Urban Areas are encouraged to include representation from additional areas that are part of the 10-mile buffer area as members of the UAWG, as appropriate, and to continue to involve contiguous jurisdictions and mutual aid partners in program implementation. The UAWG will be responsible for coordinating development and implementation of all program initiatives, including the Investment Justification, Urban Area Homeland Security Strategy development, the methodology for allocating funds (in coordination with the SAA), and any direct services that are delivered by G&T.

Furthermore, where there is a RTSWG or an Area Maritime Security Committee active within the geographical area, the UAWG should include them as functional sub-committees to their organization. G&T strongly encourages that, wherever possible, previously established local working groups be leveraged for this purpose. Local MMRS and Citizen Corps Council representatives must be included as well. An overview of the UAWG structure and a list of members and their associated jurisdictions must be provided to G&T along with the grant application.

**Urban Area Homeland Security Strategy:** Urban Areas must utilize their Urban Area Homeland Security Strategy and the State’s Program and Capability Enhancement Plan as the basis for requesting funds to support Investments identified in the Investment Justification. There must be a clear correlation between the goals, objectives, and priorities identified in the Urban Area Homeland Security Strategy and FY 2006 UASI program activities. In addition, the Urban Area Homeland Security Strategy must also be consistent with and supportive of the State Homeland Security Strategy and the Program and Capability Enhancement Plan submitted by the State as part of the FY 2006 HSGP application.

Any newly identified Urban Areas receiving funding in FY 2006 must develop an Urban Area Homeland Security Strategy. Findings from the Program and Capability Review as well as recently updated State Homeland Security Strategies can serve as a guide for the development of an Urban Area Homeland Security Strategy. This strategy must be developed jointly by all units of government in the defined Urban Area and comport with Homeland Security Strategy Guidance released in July 2005 (<http://www.ojp.usdoj.gov/odp/assessments/definition.htm>) to ensure that strategies align with the Goal. All new Urban Area Homeland Security Strategies must be completed and submitted to G&T no later than March 2, 2006, as part of their application for FY 2006 HSGP funds.

**Allocation of Funds:** The intent of the grant is to establish a metropolitan area-wide approach to homeland security. Therefore, the use and allocation of all grant funds available through the FY 2006 UASI program must focus on the investments identified in the Urban Area’s Investment Justification and the implementation of the validated Urban Area Homeland Security Strategy. The use of funds must also be consistent with the State Homeland Security Strategy, the Program and Capability Enhancement Plan, and the UASI program guidelines.

The SAA POC, in coordination with the UAWG, must develop a methodology for allocating funding available through the UASI program. The UAWG must reach consensus on funding

allocations. If consensus cannot be reached within the 60-day time period allotted for the State to obligate funds to subgrantees, the SAA must make the allocation determination. If consensus cannot be reached within the 60-day time period and the Urban Area crosses State boundaries, the SAA to whom funding has been awarded must make the allocation determination. The SAA must provide written documentation verifying consensus of the UAWG, or the failure to achieve consensus, on the allocation of funds provided through the FY 2006 UASI program. This documentation must be submitted to G&T not later than 60 days after the grant award date, and prior to the obligation or drawdown of funds. Any funds retained by the State on behalf of an Urban Area must be used in direct support of the Urban Area.

**Defining Urban Areas:** The SAA POC, in coordination with the candidate Urban Area, must fully define the Urban Area as it will apply to the FY 2006 UASI program. The identified city or combined entity represents the candidate Urban Area eligible to apply for funding under the FY 2006 UASI program. For those Urban Areas with a combined entity, that area represents the minimum area that must be part of the defined Urban Area. In defining the Urban Area for purposes of program implementation, States, in coordination with Urban Areas, are encouraged to also include additional areas that are part of the 10-mile buffer area, contiguous jurisdictions, and mutual aid partners, as appropriate.

The definition of the Urban Area is limited to jurisdictions contiguous to the geographic area used to determine eligibility, or with which jurisdictions in that area have established formal mutual aid agreements. States may request a waiver for this limitation for regions previously established by Executive Order, law or compact. For the purposes of the FY 2006 UASI program, the Washington, D.C. Urban Area will consist of the NCR as set forth in 10 U.S.C. 2674(f)(2).

In coordination with the UAWG, the SAA POC may redefine the geographic boundaries of the Urban Area as it will apply to the FY 2006 UASI program. The SAA POC must notify G&T of this change.

- For the purposes of the FY 2006 UASI program, the State may request a waiver to define Urban Areas using regions previously established by Executive Order, law or compact.
- If the Urban Area is expanded to include additional jurisdictions, those additional jurisdictions are eligible for, but not entitled to, receipt of funding through the program. All FY 2006 UASI program budget allocations must continue to support the Urban Area Homeland Security Strategy and will require consensus from the UAWG. If consensus cannot be reached, the SAA must make the allocation determination.
- Inclusion of additional jurisdictions will not lead to increased funding for the Urban Area.
- Training, planning, organizing, and exercising projects can be implemented as regional projects with or without a change to the Urban Area.

## C. Authorized Program Expenditures

Allowable expenditures for the FY 2006 UASI program comport with FY 2006 SHSP (except for the use of funds for operational costs). Please refer to Appendix D for a summary of authorized and unauthorized UASI expenditures.

### C.1. Planning

Urban Areas may use FY 2006 UASI funds for multi-discipline planning efforts to prioritize needs, update preparedness strategies, allocate resources, and deliver preparedness programs. These efforts include the collection and analysis of intelligence and information and the development of policies, plans, procedures, mutual aid agreements, strategies, and other publications that comply with relevant laws, regulations, and guidance necessary to perform assigned missions and tasks. It is explicitly permissible to use planning funds to hire government and/or contractor personnel to conduct planning activities described here.

Similar to SHSP, FY 2006 UASI funds may be used for a range of homeland security planning activities, such as:

- Developing and implementing homeland security support programs and adopting DHS national initiatives including but not limited to the following:
  - o Implementing the National Preparedness Goal and Guidance.
  - o Implementing and adopting NIMS.
  - o Modifying existing incident management and Emergency Operating Procedures (EOPs) to ensure proper alignment with the NRP coordinating structures, processes, and protocols.
  - o Establishing or enhancing mutual aid agreements.
  - o Developing communications and interoperability protocols and solutions.
  - o Conducting local, regional, and Tribal program implementation meetings.
  - o Developing or updating resource inventory assets in accordance to typed resource definitions issued by the NIC.
  - o Designing State and local geospatial data systems.
  - o Conducting public education and outreach campaigns, including promoting individual, family and business emergency preparedness; alerts and warnings education; and evacuation plans.
- Developing related terrorism prevention activities including:
  - o Planning to enhance security during heightened alerts, during terrorist incidents, and/or during mitigation and recovery.
  - o Multi-discipline preparation across first responder community, including EMS for response to catastrophic events and acts of terrorism.
  - o Public information/education: printed and electronic materials, public service announcements, seminars/town hall meetings, web postings coordinated through local Citizen Corps Councils.
  - o Citizen Corps volunteer programs and other activities to strengthen citizen participation.

- o Conducting public education campaigns, including promoting individual, family and business emergency preparedness; promoting the *Ready* campaign; and/or creating State, regional or local emergency preparedness efforts that build upon the *Ready* campaign.
- o Evaluating CIP security equipment and/or personnel requirements to protect and secure sites.
- o CIP cost assessments, including resources (financial, personnel, etc.) required for security enhancements/deployments.
  
- Developing and enhancing plans and protocols, including but not limited to:
  - o Developing or enhancing EOPs and operating procedures.
  - o Developing terrorism prevention/deterrence plans.
  - o Developing plans, procedures, and requirements for the management of infrastructure and resources related to HSGP and implementation of State or Urban Area Homeland Security Strategies.
  - o Developing or enhancing border security plans.
  - o Developing or enhancing cyber security plans.
  - o Developing or enhancing cyber risk mitigation plans.
  - o Developing or enhancing agriculture/food security risk mitigation, response, and recovery plans.
  - o Developing public/private sector partnership emergency response, assessment, and resource sharing plans.
  - o Developing or updating local or regional communications plans.
  - o Developing plans to support and assist special needs jurisdictions, such as port authorities and rail and mass transit agencies.
  - o Developing or enhancing continuity of operations and continuity of government plans.
  - o Developing or enhancing existing catastrophic incident response and recovery plans to include and integrate Federal assets provided under the NRP.
  - o Developing or enhancing evacuation plans.
  - o Developing or enhancing citizen surge capacity.
  
- Developing or conducting assessments, including but not limited to:
  - o Conducting point vulnerability assessments at critical infrastructure sites/key assets and developing remediation/security plans.
  - o Conducting cyber risk and vulnerability assessments.
  - o Conducting assessments and exercises of existing catastrophic incident response and recovery plans and capabilities to identify critical gaps that cannot be met by existing local and State resources.
  - o Activities that directly support the identification of specific catastrophic incident priority response and recovery projected needs across disciplines (e.g. law enforcement, fire, EMS, public health, behavioral health, public works, agriculture, information technology, and citizen preparedness).
  - o Activities that directly support the identification and advance preparation of pre-designated temporary housing sites.



## C.2. Organization

States and Urban Areas may use FY 2006 UASI funds to support select organization activities. States and Urban Areas must justify proposed expenditures of UASI funds to support organization activities within their Investment Justification submission using historical data and other analysis to substantiate their proposals. No more than 25 percent of the gross amount of the allocation for this program may be used for operational expenses and overtime costs for the three (3) operational activities noted below.

1. Operational overtime costs associated with increased security measures at critical infrastructure sites during periods of DHS-declared heightened alert.

**UASI:** Up to 25 percent of FY 2006 funds may be used in UASI jurisdictions.

- Of this amount, up to 10 percent may be used for costs incurred during Code Yellow or Orange.
- The remaining 15 percent may be used for costs incurred only during Code Orange.
- Operational overtime costs incurred at National Special Security Events (NSSEs) in UASI jurisdictions, as designated by the Secretary of Homeland Security, are also allowed.
- States with UASI jurisdictions can use funds retained at the State level to reimburse eligible operational overtime expenses incurred by the State (up to a maximum of 25 percent of the State share of the UASI grant). However, those activities must directly support increased security measures enacted in the UASI jurisdictions. States should be judicious in the use of Federal grant funds when protecting critical infrastructure and should leverage public/private partnerships. States should also consider the use of private assets in the protection of private facilities.

In support of these efforts for enhanced capabilities of detecting, deterring, disrupting, and preventing acts of terrorism, costs eligible for reimbursement under this policy are identical to those deemed allowable under previous Code Orange alerts. Therefore, subject to the conditions stated above, States and local governments may use FY 2006 UASI funds to support select operational expenses associated with increased security measures at critical infrastructure sites in the following authorized categories:

- Backfill and overtime expenses for staffing State or local emergency operations centers (EOCs)
- Hiring of contracted security for critical infrastructure sites
- Public safety overtime
- National Guard deployments to protect critical infrastructure sites, including all resources that are part of the standard National Guard deployment package
- Increased border security activities in coordination with CBP as outlined in Information Bulletin #135.<sup>13</sup>

<sup>13</sup> Proposed operational activities should emphasize those measures that will increase border security in direct coordination with CBP personnel. State, local, and Tribal law enforcement personnel may provide increased enforcement presence by generally increasing their patrol presence at the border; by providing additional traffic

Consumable costs, such as fuel expenses, are *not allowed* except as part of the standard National Guard deployment package.

2. Overtime costs are allowable for personnel to participate in information, investigative, and intelligence sharing activities specifically related to homeland security. This includes activities such as anti-terrorism task forces, Joint Terrorism Task Forces (JTTF), Area Maritime Security Committees (as required by the Maritime Transportation Security Act of 2002), and Terrorism Early Warning (TEW) groups.
3. Grant funds may be used towards the hiring of new staff and/or contractors to serve as intelligence analysts to support information/intelligence fusion capabilities. In order to be hired as an Intelligence Analyst, staff and/or contractor personnel must have successfully completed training to ensure baseline proficiency in *intelligence analysis and production*. Furthermore, costs associated with hiring new intelligence analysts are allowable only for the period of performance of the FY 2006 UASI and LETPP programs. Upon close-out of the FY 2006 grants, States and Urban Areas shall be responsible for supporting the sustainment costs for those intelligence analysts.

The International Association of Law Enforcement Intelligence Analysts' (IALEIA) Educational Standard # 7 (page 14 of the IALEIA Analytic Standards booklet) provides standards on the categories of training needed for intelligence analysts. These include subject-matter expertise, analytic methodologies, customer-service ethics, information handling and processing skills, critical thinking skills, computer literacy, and objectivity and intellectual honesty. Successful completion the following courses satisfies the intelligence analyst training requirement:

- Intelligence Analyst Training Program (FLETC).
- Foundations of Intelligence Analysis Training (International Association of Law Enforcements Intelligence Analysis).

Additional courses are being identified and will be shared as soon as possible. ***A certificate of completion of such training must be on file with the SAA and should be made available to Preparedness Officers upon request upon the hiring of personnel.***

---

control support at the border and at border patrol traffic checkpoints; and by enhancing their participation in the Integrated Border Enforcement Teams. This policy does not result in a change or extension of Federal authority to State, Tribal, or local law enforcement agencies to enforce Federal immigration laws. If Federal immigration violations are encountered, consistent with current practices, State, local, and Tribal agencies may refer those violations to CBP authorities for appropriate action. No funds may be obligated or drawn down in support of these activities without HQ-CBP approval of operational plans and without submission to and approval by G&T of budget detail worksheets. State, local, and Tribal law enforcement agencies shall not use this funding to supplant routine patrol and law enforcement operations or activities in order to perform other activities not directly related to providing an enhanced law enforcement presence.

**C.3. Equipment**

UASI funds may be used for equipment acquisition from the 21 equipment categories listed in the FY 2006 G&T AEL. The FY 2006 AEL is available in its entirety online through the RKB at <http://www.rkb.mipt.org> and the equipment categories are outlined in Table 9 below and Appendix D.

**Table 9 – UASI Allowable Equipment Categories**

Cat. #	Category Title	Cat. #	Category Title
[1]	Personal Protective Equipment	[12]	CBRNE Incident Response Vehicles
[2]	Explosive Device Mitigation and Remediation Equipment	[13]	Terrorism Incident Prevention Equipment
[3]	CBRNE Operational and Search and Rescue Equipment	[14]	Physical Security Enhancement Equipment
[4]	Information Technology	[15]	Inspection and Screening Systems
[5]	Cyber Security Enhancement Equipment	[16]	Agricultural Terrorism Prevention, Response and Mitigation Equipment
[6]	Interoperable Communications Equipment	[17]	CBRNE Prevention and Response Watercraft
[7]	Detection Equipment	[18]	CBRNE Aviation Equipment
[8]	Decontamination Equipment	[19]	CBRNE Logistical Support Equipment
[9]	Medical Supplies and Limited Types of Pharmaceuticals	[20]	Intervention Equipment
[10]	Power Equipment	[21]	Other Authorized Equipment
[11]	CBRNE Reference Materials		

**C.4. Training**

FY 2006 UASI funds may be used to enhance the capabilities of State and local emergency preparedness and response personnel through development of a State homeland security training program. Allowable training-related costs include:

1. Establishment of support for, conduct of, and attendance at preparedness training programs within existing training academies/institutions, universities, or junior colleges. Preparedness training programs are defined as those programs related to prevention, protection, response, and or recovery from natural, technical, or manmade catastrophic incidents, supporting one or more Target Capabilities in alignment with national priorities as stated in the Goal. Examples of such programs include but are not limited to CBRNE terrorism, critical infrastructure protection, cyber security, and citizen preparedness.
2. Overtime and backfill costs associated with attendance at G&T-sponsored and approved training courses. UASI funding may also be used for training citizens in awareness, prevention, protection, response, recovery skills

**C.5. Exercises**

All Urban Areas are required to develop a Multi-year Exercise Plan and submit it to G&T on an annual basis. While Urban Area specific, this plan must tie into the Multi-year Exercise Plan

developed by the State, and be in line with the Urban Area Homeland Security Strategy. Further, Urban Areas are encouraged to develop a Multi-year Plan and Schedule that takes into consideration anticipated training needs of the Urban Area for at least the immediate year, with exercises being timed to provide responders the opportunity to utilize training received. This combined schedule should also ensure that training and exercises complement each other. An example of a combined Multi-year Training and Exercise Plan can be found at the HSEEP Website or G&T Secure Portal. Further guidance concerning EPWs can be found in the HSEEP Volumes.

Urban Areas are eligible to apply for exercise direct support, but must do so in coordination with the SAA.

#### **C.6. Personnel**

Hiring, overtime, and backfill expenses are allowable only to perform programmatic activities deemed allowable under existing guidance. Supplanting, however, is not allowed.

Up to 15% of programmatic spending may be used to support the hiring of full or part-time personnel to conduct program activities that are allowable under the entire FY 2006 HSGP (i.e., planning, training program management, exercise program management, etc). Grantees may request that DHS issue a waiver to increase that ceiling. Waiver decisions are at the discretion of DHS and will be considered on a case-by-case basis. The ceiling on personnel costs does not apply to contractors, and is in addition to eligible M&A costs and eligible hiring of intelligence analysts. Grantees may hire staff only for program management functions not operational duties. Hiring planners, training program coordinators, exercise managers, and grant administrators fall within the scope of allowable program management functions. Grant funds may not be used to support the hiring of sworn public safety officers to fulfill traditional public safety duties.

#### **C.7. Management and Administration**

No greater than 5 percent of the UASI allocation may be used for M&A. Local jurisdiction subgrantees may retain and use up to 3 percent of their subaward from the State for local M&A purposes. States may pass through a portion of the State M&A allocation to local subgrantees in order to supplement the 3 percent M&A allocation allowed on subgrants. However, no more than 5 percent of the total subaward may be expended by subgrantees on M&A costs.

**VIII. LAW  
ENFORCEMENT  
TERRORISM  
PREVENTION  
PROGRAM**

## VIII. LAW ENFORCEMENT TERRORISM PREVENTION PROGRAM

### A. Program Overview

LETPP specifically focuses upon the prevention of terrorist attacks and provides law enforcement and public safety communities working with their private partners' funds to support the following activities: intelligence gathering and information sharing through enhancing/establishing fusion centers; hardening high value targets; planning strategically; continuing to build interoperable communications; and collaborating with non-law enforcement partners, other government agencies and the private sector. LETPP funds should be focused on enhancing the Target Capabilities unique to terrorism.

#### Target Capabilities

- Planning
- Communications
- Information Gathering and Recognition of Indicators & Warnings
- Law Enforcement Investigation and Operations
- Intelligence Analysis and Production
- CBRNE Detection
- Intelligence/Information Sharing & Dissemination
- Critical Infrastructure Protection

The SAA must coordinate the implementation of this program with the State's Lead Law Enforcement Agency (LLEA).

When identifying administrative and planning needs, each grantee should assess current staffing levels and determine whether a portion of the FY 2006 LETPP funds should be used to enhance administrative capabilities within the LLEA.

### B. LETPP and the National Preparedness Goal

LETPP centers on prevention efforts, one of the four core homeland security mission areas. Prevention efforts are critical to effective State and local implementation of the Goal. Funds awarded under this program directly support several of the Target Capabilities in the Goal. These include Information Gathering and Recognition of Indicators & Warnings, Law Enforcement Investigation and Operations, Intelligence Analysis and Production, CBRNE Detection, Intelligence/Information Sharing & Dissemination, and Critical Infrastructure Protection.

### C. Authorized Program Expenditures

FY 2006 LETPP funding is expended based on the State Homeland Security Strategies. Please refer to Appendix D for additional information on authorized and unauthorized LETPP expenditures.

#### C.1. Planning

LETPP funds may be used for a range of law enforcement terrorism prevention planning activities, including the following:

- Developing and planning for information/intelligence sharing groups.
- Conducting point vulnerability analyses and assessments.
- Soft target security planning (public gatherings).

- Developing border security operations plans in coordination with CBP.
- Developing, implementing, and reviewing Area Maritime Security Plans for ports, waterways, and coastal areas.
- Updating and refining threat matrices.
- Acquiring systems allowing connectivity to Federal data networks, such as National Crime Information Center (NCIC) and Integrated Automated Fingerprint Identification System (IAFIS), as appropriate.
- Designing and developing State and local geospatial data systems.
- Costs associated with the implementation and adoption of NIMS.
- Developing related terrorism prevention activities including:
  - Planning for enhancing security during heightened alerts, terrorist incidents, and/or mitigation and recovery.
  - Public information/education: printed and electronic materials, public service announcements, seminars/town hall meetings, web postings.
  - Citizen Corps volunteer programs and other activities to strengthen citizen participation.
  - Evaluating CIP security equipment and/or personnel requirements to protect and secure sites.

## C.2. Organization

States and Urban Areas may use FY 2006 LETPP funds to support select organization activities. States and Urban Areas must justify proposed expenditures of LETPP funds to support organization activities within their Investment Justification submission using historical data and other analysis to substantiate their proposals. No more than 25 percent of the gross amount of the allocation for this program may be used for operational expenses and overtime costs for the three operational activities noted below.

1. Operational overtime costs associated with increased security measures at critical infrastructure sites during DHS-declared periods of heightened alert.

**LETTP:** Up to 25 percent of FY 2006 LETPP funds may be used for costs incurred during Code Orange. Costs associated with **border protection activities only** are also eligible at Code Yellow, provided that those activities are conducted in accordance with previous guidance issued in Information Bulletin #135 and outlined below. These activities must be coordinated with CBP.

In support of these efforts for enhanced capabilities of detecting, deterring, disrupting, and preventing acts of terrorism, costs eligible for reimbursement under this policy are identical to those deemed allowable under previous Code Orange alerts. Therefore, subject to the conditions stated above, States and local governments may use FY 2006 LETPP funds to support select operational expenses associated with increased security measures at critical infrastructure sites in the following authorized categories:

- Backfill and overtime expenses for staffing State or local emergency operations centers (EOCs).

- Hiring of contracted security for critical infrastructure sites.
- Public safety overtime.
- National Guard deployments to protect critical infrastructure sites, including all resources that are part of the standard National Guard deployment package.
- Increased border security activities in coordination with CBP, as outlined in Information Bulletin #135.<sup>14</sup>

Consumable costs, such as fuel expenses, are *not allowed* except as part of the standard National Guard deployment package.

2. Overtime costs are allowable for personnel to participate in information, investigative, and intelligence sharing activities specifically related to homeland security. This includes activities such as anti-terrorism task forces, Joint Terrorism Task Forces (JTTF), Area Maritime Security Committees (as required by the Maritime Transportation Security Act of 2002), and Terrorism Early Warning (TEW) groups.
3. Grant funds may be used towards the hiring of new staff and/or contractors to serve as intelligence analysts to support information/intelligence fusion capabilities. In order to be hired as an Intelligence Analyst, staff and/or contractor personnel must have successfully completed training to ensure baseline proficiency in *intelligence analysis and production*. Furthermore, costs associated with hiring new intelligence analysts are allowable only for the period of performance of the FY 2006 UASI and LETPP programs. Upon close-out of the FY 2006 grants, States and Urban Areas shall be responsible for supporting the sustainment costs for those intelligence analysts.

The International Association of Law Enforcement Intelligence Analysts' (IALEIA) Educational Standard # 7 (page 14 of the IALEIA Analytic Standards booklet) provides standards on the categories of training needed for intelligence analysts. These include subject-matter expertise, analytic methodologies, customer-service ethics, information handling and processing skills, critical thinking skills, computer literacy, and objectivity and intellectual honesty. Successful completion the following courses satisfies the intelligence analyst training requirement:

- Intelligence Analyst Training Program (FLETC).
- Foundations of Intelligence Analysis Training (International Association of Law Enforcements Intelligence Analysis).

---

<sup>14</sup> Proposed operational activities should emphasize those measures that will increase border security in direct coordination with CBP personnel. State, local, and Tribal law enforcement personnel may provide increased enforcement presence by generally increasing their patrol presence at the border; by providing additional traffic control support at the border and at border patrol traffic checkpoints; and by enhancing their participation in the Integrated Border Enforcement Teams. This policy does not result in a change or extension of Federal authority to State, Tribal, or local law enforcement agencies to enforce Federal immigration laws. If Federal immigration violations are encountered, consistent with current practices, State, local, and Tribal agencies may refer those violations to CBP authorities for appropriate action. No funds may be obligated or drawn down in support of these activities without HQ-CBP approval of operational plans and without submission to and approval by G&T of budget detail worksheets. State, local, and Tribal law enforcement agencies shall not use this funding to supplant routine patrol and law enforcement operations or activities in order to perform other activities not directly related to providing an enhanced law enforcement presence.



Additional courses are being identified and will be shared as soon as possible. *A certificate of completion of such training must be on file with the SAA and should be made available to Preparedness Officers upon request upon the hiring of personnel.*

**C.3. Equipment**

LETTP funds may be used for equipment acquisition from the LETTP equipment categories listed in the FY 2006 G&T AEL. The FY 2006 AEL is available in its entirety online through the RKB at <http://www.rkb.mipt.org> and the equipment categories are outlined in Table 10 below and Appendix D.

**Table 10 – LETTP Allowable Equipment Categories**

Cat. #	Category Title	Cat. #	Category Title
[1]	Personal Protective Equipment	[12]	CBRNE Incident Response Vehicles
[2]	Explosive Device Mitigation and Remediation Equipment	[13]	Terrorism Incident Prevention Equipment
[3]	CBRNE Operational and Search and Rescue Equipment	[14]	Physical Security Enhancement Equipment
[4]	Information Technology	[15]	Inspection and Screening Systems
[5]	Cyber Security Enhancement Equipment	[17]	CBRNE Prevention and Response Watercraft
[6]	Interoperable Communications Equipment	[19]	CBRNE Logistical Support Equipment
[10]	Power Equipment	[20]	Intervention Equipment
[11]	CBRNE Reference Materials	[21]	Other Authorized Equipment

**C.4. Training**

LETTP funds may be used for a range of law enforcement terrorism prevention related training activities to enhance the capabilities of State and local personnel, including the following:

- Training courses on building information sharing capacities.
- Training that includes methods of target hardening.
- Training for facility security personnel.
- Training for vessel and port law enforcement security personnel recognition of CBRNE, agriculture, and cyber threats.
- NIMS training.
- Weaponization of CBRNE, agriculture, and cyber threats.
- History of terrorism and social environments contributing to threats.
- Surveillance and counter-surveillance techniques.
- Identifying/assessing critical infrastructure assets, vulnerabilities, and threats.
- Intelligence analysis.
- Cyber security protective measures training.
- Multi-cultural training for undercover operations.
- Language training.
- Joint training with other homeland security entities (e.g., U.S. Secret Service, Customs

and Border Protection).

- Training on the use of interoperable communications equipment.
- CIP training.
- Training associated with the collection, analysis, mapping, integration, and dissemination of geospatial data and imagery.
- Geospatial database use, design, development, and management training.
- Agricultural/food security-related training.
- Training for citizens in terrorism awareness and for volunteer participation to support law enforcement activities, to include the Volunteers in Police Service and Neighborhood Watch programs.

Multi-level training should be focused on a regional model. Grantees using these funds to develop their own courses should address the critical training areas and gaps identified in the State's Homeland Security Strategy and must adhere to the *G&T Emergency Responder Guidelines* and *G&T Homeland Security Guidelines on Prevention and Deterrence*. Training should address specific capabilities and related tasks articulated in the TCL and the UTL. It should also comport with all applicable Federal, State and local regulations, certifications, guidelines and policies deemed appropriate for the type and level of training.

#### **C.5. Exercises**

LETPP funds may be used to design, develop, conduct, and evaluate terrorism prevention-related exercises, including the following:

- Exercises to evaluate the effectiveness of information sharing plans, policies, procedures and protocols.
- Exercises to evaluate NIMS implementation.
- Exercises to evaluate facility and/or vessel security protection.
- Exercises to evaluate area maritime security protection.
- Exercises to evaluate threat recognition capabilities.
- Exercises to evaluate cyber security capabilities.
- Exercises to evaluate agricultural/food security capabilities.
- Exercises to evaluate prevention readiness and techniques.
- “Red Team” (force on force) exercises.
- Interoperable communications exercise.
- Critical infrastructure vulnerability, protection, and/or attack exercises.

Where practical, these exercises should involve the public sector, non-governmental partners, trained citizen volunteers, and the general public. State and local governments should work with their Citizen Corps Councils to include volunteers from programs such as Volunteers in Police Service, Neighborhood Watch, and the general public.

#### **C.6. Personnel**

Hiring, overtime, and backfill expenses are allowable only to perform programmatic activities deemed allowable under existing guidance. Supplanting, however, is not allowed.

Up to 15% of programmatic spending may be used to support the hiring of full or part-time personnel to conduct program activities that are allowable under the entire FY 2006 HSGP (i.e., planning, training program management, exercise program management, etc). Grantees may request that DHS issue a waiver to increase that ceiling. Waiver decisions are at the discretion of DHS and will be considered on a case-by-case basis. The ceiling on personnel costs does not apply to contractors, and is in addition to eligible M&A costs and eligible hiring of intelligence analysts. Grantees may hire staff only for program management functions not operational duties. Hiring planners, training program coordinators, exercise managers, and grant administrators fall within the scope of allowable program management functions. Grant funds may not be used to support the hiring of sworn public safety officers to fulfill traditional public safety duties.

#### **C.7. Management and Administration**

No more than 5 percent of the LETPP allocation may be used for M&A. Local jurisdiction subgrantees may retain and use up to 3 percent of their subaward from the State for local M&A purposes. States may pass through a portion of the State M&A allocation to local subgrantees in order to supplement the 3 percent M&A allocation allowed on subgrants. However, no more than 5 percent of the total subaward may be expended by subgrantees on M&A costs.

# **IX. METROPOLITAN MEDICAL RESPONSE SYSTEM**

## IX. METROPOLITAN MEDICAL RESPONSE SYSTEM

### A. Program Overview

The FY 2006 MMRS program provides funding to designated localities to assist in writing plans, developing training, purchasing equipment and pharmaceuticals, and conducting exercises to achieve the Target Capabilities necessary to respond to a mass casualty event, whether caused by a WMD terrorist act, epidemic disease outbreak, natural disaster, or HAZMAT accident, during the crucial first hours of a response until significant external assistance can arrive and become operational.

MMRS establishes linkages among emergency responders, medical treatment resources, public health officials, emergency management offices, volunteer organizations and other local elements working together to reduce the mortality and morbidity that would result from a catastrophic incident. The MMRS program also emphasizes enhanced mutual aid with neighboring localities (MMRS “Operational Area”) and State and Federal agencies. Additional information is provided at <http://mmrs.fema.gov>.

The FY 2006 MMRS Program will support the MMRS jurisdictions in:

- Achieving preparedness in the MMRS-related Capability Focus Areas, which supports efforts to implement the Goal.
- Ensuring that their strategic goals, objectives, operational capabilities, and resource requirements are adequately incorporated in State and Urban Area Homeland Security Assessment and Strategy documents.
- Revising their operational plans to reflect State and Urban Area Homeland Security Assessments and Strategies.
- Ensuring the maintenance of MMRS capabilities established through the completion of baseline deliverables and other previous activities supported by Federal funding.

#### A.1. Period of Performance

The period of performance for MMRS is 24 months from the award date. A portion of this period overlaps with deliverable schedules under FY 2004 and FY 2005 MMRS grants. Grant recipients, to the greatest extent possible, should correlate the funding from FY 2006 MMRS

#### Target Capabilities

- Planning
- Community Preparedness and Participation
- Communications
- Information Gathering and Recognition of Indicators & Warnings
- CBRNE Detection
- Epidemiological Surveillance & Investigation
- Public Health Laboratory Testing
- Citizen Protection: Evacuation and/or In-Place Protection
- Isolation & Quarantine
- Critical Resource Logistics & Distribution
- Urban Search & Rescue
- Emergency Public Information & Warning
- Responder Health & Safety
- Triage & Pre-Hospital Treatment
- Public Safety & Security Response
- Medical Surge
- Medical Supplies Management & Distribution
- Environmental Health
- Mass Prophylaxis
- Mass Care
- Firefighting Operations/Support
- Fatality Management
- WMD/Hazardous Materials Response & Decontamination

Program with the ongoing activities funded by the previous years vehicles to determine the best allocation of funds between ongoing and new initiatives.

## **B. MMRS and the National Preparedness Goal**

The MMRS program purpose and guidance, and the capability achievements of MMRS jurisdictions, create extensive and essential relevance of MMRS to the Goal, National Priorities, and numerous Target Capabilities, (see Appendix G).

MMRS jurisdictions, where prior years program guidance has been appropriately implemented, have already established significant capabilities in integrated mass casualty preparedness for CBRNE incidents, whether human caused, naturally occurring, or the result of an accident. These capability achievements should provide a significant foundation for further increasing capabilities as required by the implementation of the Goal.

Accordingly, the MMRS Steering Committees and component functional leaders are expected to make essential contributions to the achievement of these Target Capabilities, in their home political jurisdictions and affiliated jurisdictions constituting their MMRS Operational Area, their Urban Area, and throughout their State(s).

## **C. Program Requirements**

All provisions of the FY 2006 HSGP Program Guidelines, Sections I through V, and appendices, apply to MMRS unless explicitly stated otherwise herein.

MMRS jurisdictions are strongly encouraged to use G&T services regarding: the preparation and implementation of homeland security assessments and strategies, technical assistance, training programs, and the Homeland Security Exercise and Evaluation Program. G&T Preparedness Officers will serve as the principal POCs for MMRS jurisdictions in accessing these services. Other DHS-provided support relevant to MMRS capabilities enhancement includes the NIC and the Office for Interoperability and Compatibility (OIC).

### **C.1. Allocation of Funds**

Recognizing that MMRS is inherently multi-jurisdictional, funds must be expended to support the regional MMRS to establish and sustain enhanced local capabilities. States are encouraged to pass through 100 percent of grant funds, but may retain 20 percent to facilitate strategy assessment and capability integration between the State and MMRS jurisdictions. States must have written concurrence between the SAA and MMRS Steering Committee Chair to use funds to:

- Support regional MMRS Operational Areas overall.
- Advise and assist MMRS jurisdictions in awareness of, and in providing input to, State and Urban Area Homeland Security Assessments and Strategies.
- Ensure that MMRS-related mutual aid agreements conform with Statewide and State regional resource management requirements and capabilities.

- Advise and assist MMRS jurisdictions with HSPD-8 preparedness assessments and reporting.

States are reminded that MMRS funds must be expended to support efforts to establish and sustain enhanced local capabilities in MMRS jurisdictions so that those jurisdictions are prepared to respond to any mass casualty incident, including terrorism, disease outbreaks, natural disasters, and large scale hazardous materials accidents. The intent of the MMRS program is to enhance these capabilities at the local level so that these jurisdictions can manage the aftermath of an incident until significant external assistance can arrive. MMRS jurisdictions may choose to allocate funding to the State to assist them in developing these capabilities. The MMRS Steering Committee Chair must provide written concurrence for the State to retain funds for these program purposes. Further, the MMRS jurisdictions have discretion to determine what level of funding, if any, they will allow the States to retain. As such, the MMRS jurisdictions are not constrained by the 20 percent cap on State retention of MMRS funds indicated in the program guidance.

## **C.2. Revised Capability Focus Areas (CFA)**

The listing constitutes revised MMRS Capability Focus Areas (CFAs) and reflects the correlation of the Goal, National Priorities and TCL, and updates the FY 2004 and 2005 MMRS CFAs. The Target Capabilities constitute the primary guidance for the MMRS activities engaged in achieving these capabilities. Reference to previous and continuing MMRS program guidance is also incorporated. MMRS jurisdictions have the option of using grant funds to improve capabilities in any of the other Target Capabilities listed in the MMRS column of Appendix G.

MMRS jurisdictions must also sustain enhanced capabilities achieved through the implementation of prior years' program guidance and funding.

### ***CFA 1 - Strengthen Medical Surge***

This CFA links to the Medical Surge Target Capability. MMRS jurisdictions are strongly encouraged to develop, in conjunction with State and Urban Area officials, altered standards of care authorities and guides, based on the information provide in the AHRQ report, "Altered Standards of Care in Mass Casualty Events" (pub. No. 05-0043, April 2005).

Elements of the MMRS baseline capabilities apply to this area, including the WMD CBRNE plans and Local Hospital and Regional Healthcare Systems Plan. The provisions of FY 2004 and FY 2005 CFA 2, "ensure operational viability of mass care shelters and medical treatment facilities" are incorporated into this CFA:

- Revise or update current plans to include the provision of hazardous/toxic substances portal and point detection and monitoring, decontamination and public safety support to mass care shelters and medical treatment facilities by designated personnel and equipment.
- Consider the establishment of reception centers, which consolidate monitoring, triage, decontamination, and registration of affected persons.

- Identify agent antidotes by types and dosage volumes and planning for storage, dispersal, and dispensing, and awareness of how agent antidote dosages may impact the health of vulnerable populations (e.g., immune-suppressed individuals, children).
- Ensure that alternate medical treatment facilities have immediately available electric power, water and sewer, environmental controls, and other necessary infrastructure support to become operationally viable on short notice.

### ***CFA 2 - Strengthen Mass Prophylaxis***

This CFA links to the Mass Prophylaxis Target Capability. MMRS jurisdictions should ensure that all sources of medicines and medical supplies (e.g., MMRS cache, CHEMPACK, and HRSA-funded hospital-based caches), necessary to protect first responders and first receivers and support their continued operations in hazardous environments, and to provide mass prophylaxis, are aggregated into a NIMS-compliant master resource list and management system, in support of a mass prophylaxis distribution plan, which also addresses SNS provided items, for their Operational Area. The provisions of former CFA 8, “Pharmaceutical Cache Management and Status Reporting” are also incorporated into this CFA.

In support of CDC’s Cities Readiness Initiative, all MMRS jurisdictions which are in Urban Areas must update their mass prophylaxis plans to be able to provide for the distribution of pharmaceuticals to their entire population within 48 hours of receiving an allocation from the Strategic National Stockpile. In addition, all MMRS jurisdictions must maintain on file an inventory of the MMRS local pharmaceutical cache, in Microsoft® Excel format, to be provided electronically to DHS upon request. This inventory must include the following data elements:

- Pharmaceutical products contained and inventory of jurisdiction’s pharmaceutical cache in units of dosage.
- Names and official titles of individuals authorized to release cache pharmaceuticals.
- Each product’s Lot Number, cost, and expiration date.
- Pharmaceutical storage management and conditions, including percentage stored in hospitals and other fixed facilities, and percentage forward-deployed on emergency responder vehicles.

### ***CFA 3 - Strengthen CBRNE Detection, Response, and Decontamination Capabilities***

This CFA links to the WMD/Hazardous Materials Response and Decontamination Target Capability. Elements of MMRS baseline capabilities in CBRNE response plans are applicable to this CFA. The decontamination items in CFA 1, above, also apply to this CFA.

### ***CFA 4 - Strengthen Interoperable Communications Capabilities***

This CFA links to the Interoperable Communications Target Capability. In consideration of Katrina/Rita after-action lessons learned, in addition to the interoperable communications guidance provided in the general section of this grant guidance, in each MMRS Operational Area, there must be established a Minimum Essential Emergency Medical Communications Network (MEEMCN) capable of processing voice and data communications which is not dependent on the Public Switched Network, avoiding to the maximum extent possible reliance on terrestrial fixed site components which are vulnerable to disruption or destruction by terrorist act or natural disaster. The MEEMCN shall, at a minimum, include selected medical treatment



facilities, public health Departments, emergency operations center, public safety Department, emergency medical and law enforcement dispatch centers, and State National Guard nodes.

Network design and communications operations planning must be integrated with Urban Area, and State communications upgrade activities, and should be conducted in consultation with DHS assistance resources, including the Interoperable Communications Technical Assistance Program.

***CFA 5 - Strengthen Information Sharing and Collaboration Capabilities***

This CFA links to the National Priority for Information Sharing and Collaboration.

***CFA 6 - Expand Regional Collaboration***

This CFA links to the National Priority for Regional Collaboration and all Target Capabilities. Previous MMRS guidance applicable to this CFA includes deliverable four of the FY 2003 MMRS Contract, and the capabilities sustainment element of the FY 2004 MMRS grant guidance.

The term “MMRS Operational Area” means all of the political jurisdictions and special jurisdictions (such as port authorities and transportation authorities) with which an MMRS jurisdiction has mutual aid agreements and other preparedness and response coordination and/cooperation arrangements. This term is meant to avoid the confusion caused by the existence of multiple special purpose “regions” (e.g., emergency management, public health, homeland security, transportation/highway) in most States. The jurisdictions in an MMRS Operational Area which receive MMRS grants funds are “principal MMRS jurisdictions” and the other jurisdictions in the operational area are “affiliated MMRS jurisdictions.”

Grant funding is available to support continuing, and newly established MMRS Operational Areas. This multi-jurisdictional approach is a hallmark of the MMRS Program and achieves efficiency and economy by providing protection for a greater at-risk population, and by incorporating more highly trained response personnel (e.g., hospitals) and special-purpose resources (e.g., pharmaceuticals, equipment).

- States with two or more MMRS jurisdictions shall achieve formalized State-wide mass casualty preparedness and response capabilities.
- MMRS jurisdictions with Operational Areas in two or more States shall achieve common response protocols; common, or compatible, credentialing and permissions for first responder and medical treatment personnel; and common interoperable communications capabilities.

***CFA 7 - Triage and Pre-Hospital Treatment***

Elements of MMRS baseline capabilities in WMD CBRNE response plans are applicable to this CFA.

***CFA 8 - Medical Supplies Management and Distribution***

Activities under this CFA must implement NIMS resources management requirements, support mutual aid agreements with respect to medical treatment facilities and medical services for mass

care shelter residents, and include the consideration of the essentiality of airborne delivery of supplies to areas where ground transportation infrastructure is vulnerable to heavy damage and/or obstruction.

***CFA 9 - Mass Care (Sheltering, Feeding, and Related Services)***

Elements of former CFA 2, “Ensure operational viability of mass care shelters and medical treatment facilities” are incorporated into this CFA:

- Revise or update current plans to include the provision of hazardous/toxic substances portal and point detection and monitoring, decontamination and public safety support to mass care shelters and medical treatment facilities by designated personnel and equipment.
- Consider the establishment of reception centers, which consolidate monitoring, triage, decontamination, and registration of affected persons.
- Identify agent antidotes by types and dosage volumes and planning for storage, dispersal, and dispensing, and awareness of how agent antidote dosages may impact the health of vulnerable populations (e.g., immune-suppressed individuals, children).
- Consider the needs of individuals with disabilities and those who require continued medical maintenance to maintain their health when establishing sheltering and reception centers.

***CFA 10 – Emergency Public Information and Warning***

Former CFA 3 applies to this CFA. Review and revise planning for pre-event emergency public information message content scripting/templates and arrangements for multiple modes of message dissemination. Ensure that the distinctive characteristics of radiological, biological, and chemical agents are reflected in template messages and that self-help contamination avoidance and decontamination actions are also included. Review and revise planning for pre-event emergency public information message content scripting/templates and arrangements for multiple modes of message dissemination including accessible communication for individuals with hearing and vision disabilities.

***CFA 11 – Fatality Management***

This CFA links to the Target Capability for Fatality Management.

***CFA 12 – Volunteer Management and Donations***

This CFA links to the Target Capability for Volunteer Management and Donations.

***Pandemic Influenza Preparedness***

The updated version of the HHS Pandemic Influenza Plan was issued on November 1, 2005 and is available on-line at <http://www.hhs.gov/pandemicflu/plan/>.

As stated in the *National Strategy for Pandemic Influenza*:

Preparing for a pandemic requires the leveraging of all instruments of national power, and coordinated action by all segments of government and society. Influenza viruses do not respect the distinctions of race, sex, age, profession or nationality, and are not

constrained by geographic boundaries. The next pandemic is likely to come in waves, each lasting months, and pass through communities of all size across the Nation and world. While a pandemic will not damage power lines, banks or computer networks, it will ultimately threaten all critical infrastructure by removing essential personnel from the workplace for weeks or months.

This makes a pandemic a unique circumstance necessitating a strategy that extends well beyond health and medical boundaries, to include the sustainment of critical infrastructure, private-sector activities, the movement of goods and services across the Nation and the globe, and economic and security considerations. The uncertainties associated with influenza viruses require that our *Strategy* be versatile, to ensure that we are prepared for any virus with pandemic potential, as well as the annual burden of influenza that we know we will face.

The HHS Plan, “Public Health Guidance on Pandemic Influenza for State and Local Partners,” Section 2 provides that:

An effective local response will depend on pre-established partnerships and collaborative planning by public health officials, hospital administrators, and community leaders, who have considered a range of best-case and worst-case scenarios. It will require flexibility and real-time decision-making, guided by epidemiologic information on the pandemic virus. It will also depend on a well-informed public that understands the dangers of pandemic influenza and accepts the potential need for control measures like self-isolation and quarantine that prevent disease spread by reducing social contact. The public must also understand and accept the rationale in prioritizing the use of limited supplies of antiviral drugs and initial stocks of vaccines.

The MMRS purpose, partnerships, guidance, and capabilities achieved by MMRS jurisdictions provide a proven and established foundation for this collaborative planning.

Accordingly, as an overarching requirement for MMRS jurisdictions is the revision and updating of Continuity of Operations for emergency medical, mental health, and public health functions, and their supporting infrastructure, throughout their Operational Area. Key aspects of this activity include:

- Reviewing mutual aid agreements to ensure that they include the sharing of facilities, personnel, equipment and supplies, to include provisions for closing facilities when their key resources are decremented to the point of non-viability and making available their able personnel and remaining supplies and equipment to facilities which are viable.
- Priority dispensing of influenza vaccine and anti-viral medication to first responders and first receivers
- Providing enhanced public safety protection of mass casualty response facilities and resources
- Establishing legal authorities incorporating Altered Standards of Care

***Capabilities Documentation***

MMRS jurisdictions were required, in the FY 2003 MMRS contract statement of work, to provide an Inventory of Capabilities. MMRS jurisdictions shall update and revise those inventories (or submit their initial inventories) by reformatting them, and adding information as necessary, to address the Target Capabilities included in section D., below, to include capability assessments and needs assessments, in accordance with the Goal. The initial updated Inventory of Capabilities is required by June 30, 2006, and every six months thereafter, to be submitted along with the Biannual Strategy Implementation Reports,

**C.3. Medical Reserve Corps**

The Medical Reserve Corps (MRC) program is administered by the Office of the Surgeon General and is a key source for volunteers to support mass casualty incidents. MMRS jurisdictions are encouraged to establish and support MRC units. Up to \$25,000 per MMRS jurisdiction may be used to support local MRC units.

MRC units are community-based and are composed of local volunteer medical and public health professionals, as well as others without health backgrounds. These groups supplement existing emergency response capabilities and contribute to meeting the public health needs of the community throughout the year. MRC units are not intended to replace or substitute for local, existing emergency response systems. The local MRC unit provides an organized framework to identify, credential, train, and prepare volunteers.

The following are examples of the types of allowable expenses that MMRS jurisdictions may consider when supporting/establishing MRC units:

- Organizing the MRC unit, including establishment of a leadership and management structure (through hiring of full or part-time staff or contractors/consultants).
- Implementing mechanisms to assure appropriate integration and coordination with existing local emergency response and health assets and capabilities (including provision of legal protections for volunteers).
- Developing plans to organize and mobilize the MRC unit in response not only to urgent needs but also to address other public health needs in the community.
- Recruiting volunteers for the MRC unit.
- Credentialing MRC volunteers.
- Training MRC volunteers.
- Equipping MRC volunteers.

**D. Authorized Program Expenditures****D.1. Planning**

MMRS funds can support planning activities associated with, but not limited to:

***Homeland Security Strategy Integration***

Jurisdiction should ensure that MMRS strategic goals, objectives, operational capabilities, and resource requirements adequately reflect the State and Urban Area Homeland Security Strategy. Coordination with State and Urban Area operational plans and procedures should also occur.

***NRP and National Preparedness Goal***

MMRS jurisdictions should update/modify their operational plans and training and exercise activities as necessary to achieve conformance with the National Preparedness Goal and the NRP, to include coordinating structures, processes, and protocols.

**D.2. Organization**

Organization costs are not allowed under MMRS.

**D.3. Equipment**

MMRS funds may be used for equipment acquisition from the MMRS equipment categories listed in the FY 2006 G&T AEL. The FY 2006 AEL is available in its entirety online through the RKB at <http://www.rkb.mipt.org> and the equipment categories are outlined in Table 11 below and Appendix D.

**Table 11 – MMRS Allowable Equipment Categories**

Cat. #	Category Title	Cat. #	Category Title
[1]	Personal Protective Equipment	[10]	Power Equipment
[3]	CBRNE Operational and Search and Rescue Equipment	[11]	CBRNE Reference Materials
[4]	Information Technology	[12]	CBRNE Incident Response Vehicles
[5]	Cyber Security Enhancement Equipment	[15]	Inspection and Screening Systems
[6]	Interoperable Communications Equipment	[16]	Agricultural Terrorism Prevention, Response and Mitigation Equipment
[7]	Detection Equipment	[19]	CBRNE Logistical Support Equipment
[8]	Decontamination Equipment	[21]	Other Authorized Equipment
[9]	Medical Supplies and Limited Types of Pharmaceuticals		

**D.4. Training**

Training activities related to improving conformance with the Goal are allowed.

**D.5. Exercises**

***Exercise Costs Guidance***

Exercises conducted with G&T support (grant funds or direct support) must be managed and executed in accordance with the Homeland Security Exercise and Evaluation Program (HSEEP). The HSEEP Volumes contain guidance and recommendations for designing, developing, conducting, and evaluating exercises, as well as sample exercise materials. All HSEEP Volumes can be found at the HSEEP website (<http://hseep.dhs.gov>).

***Exercise Plan Workshop***

States must conduct an annual Training and Exercise Plan Workshop to examine the progress and effectiveness of the current exercise strategy and program. A Multi-year Training and

Exercise Plan will be produced from the workshop and submitted to G&T through the G&T Secure Portal located at <https://odp.esportals.com>.

States are encouraged to develop a Multi-year Plan and Schedule that takes into consideration anticipated training needs of the State for at least the immediate year, with exercises being timed to provide responders the opportunity to utilize training received. This combined schedule should also ensure that training and exercises complement each other. The purpose of this combined approach is to coordinate training and exercises for the State, and to ensure the scheduling of both training and exercises which are based on national and State priorities and their associated capabilities as found in the TCL. An example of a combined Multi-year Training and Exercise Plan can be found at the HSEEP Website or the G&T Secure Portal. Further guidance concerning Training and Exercise Plan Workshops can be found in the HSEEP Volumes.

### ***Exercise Scenarios***

The scenarios used in MMRS exercises must focus on catastrophic incidents with national impact (i.e. catastrophic natural hazard, terrorist incident.). The parameters for what is considered a catastrophic national impact exercise scenario is outlined in the FY 2006 Program Guidance, Section D: Allowable Cost. Grantees are allowed flexibility to develop exercise scenarios that apply to their jurisdiction within these parameters with a focus on medical issues related to preparedness and response, and should be targeted to the MMRS Capability Focus Areas provided above.

Grantees that need further clarification on exercise development, conduct, or scenarios should consult with their G&T Exercise Manager for assistance and/or approval. Citizen participation in exercises is strongly encouraged and should be coordinated with local Citizen Corps Councils. Citizen roles and responsibilities to include, but not limited to, backfilling non-professional tasks for first responders deployed on exercise planning and implementation, providing simulated victims, press, and members of the public; functioning in a range of surge capacity roles; and participating in the after-action review.

### ***CDC Public Health Emergency Preparedness Cooperative Agreement Exercise Requirement***

The FY 2005 CDC PHEP Cooperative Agreement Guidance provides, under “Additional Requirements”:

*During the award year, awardees ability to respond to events will be evaluated through assessments, site visits, drills, exercises, and responses to real events. In year one of this cooperative agreement, CDC will initiate a series of drills to test components of a comprehensive response system. In years 2-5 of this cooperative agreement, CDC will require the demonstration of a broader set of measures that are consistent with the TCLs through full-scale exercises at the State and local level. Further guidance on the development and evaluation of exercises and drills will be forthcoming from CDC. To the extent possible, public health exercises should use standards set by the DHS Homeland Security Exercise Evaluation Program (HSEEP) as well as other recognized exercise programs including those used by the Federal Emergency Management Agency (FEMA) Emergency*

*Management Institute. These exercises should test both horizontal and vertical integration with response partners at the Federal, State, local, and Tribal level.*

This requirement is not intended to be duplicative of other existing exercise requirements. MMRS jurisdictions, in coordination with the Urban Area Working Group, where relevant, other jurisdictions and organizations within their MMRS Operational Area, State level, and multi-State, organizations, are expected to schedule, design, conduct and evaluate mass casualty exercises which are in compliance with both DHS and CDC exercise requirements and guidance.

### ***Exercise Evaluation***

All exercises, whose purpose is to enhance MMRS relevant Target Capabilities, and which involve MMRS plans, procedures, organizations, personnel, and/or equipment, will be performance-based and evaluated. An After Action Report/ Improvement Plan (AAR/IP) will be prepared and submitted to G&T following every exercise, regardless of type or scope. AAR/IPs must be provided to G&T within 60 days following completion of each exercise (see HSEEP Volume IV for sample AAR/IP template). Currently, these AAR/IPs can be submitted through the G&T Secure Portal. However, G&T is working with other agencies to develop a national reporting system.

### **D.6. Personnel**

Hiring, overtime, and backfill expenses are allowable only to perform programmatic activities deemed allowable under existing guidance. Supplanting, however, is not allowed.

Up to 15% of programmatic spending may be used to support the hiring of full or part-time personnel to conduct program activities that are allowable under the entire FY 2006 HSGP (i.e., planning, training program management, exercise program management, etc). Grantees may request that DHS issue a waiver to increase that ceiling. Waiver decisions are at the discretion of DHS and will be considered on a case-by-case basis. The ceiling on personnel costs does not apply to contractors, and is in addition to eligible M&A costs and eligible hiring of intelligence analysts. Grantees may hire staff only for program management functions not operational duties. Hiring planners, training program coordinators, exercise managers, and grant administrators fall within the scope of allowable program management functions. Grant funds may not be used to support the hiring of sworn public safety officers to fulfill traditional public safety duties.

### **D.7. Management and Administration**

No greater than 5 percent of the MMRS allocation may be used for M&A. Local jurisdiction subgrantees may retain and use up to 3 percent of their subaward from the State for local M&A purposes. States may pass through a portion of the State M&A allocation to local subgrantees in order to supplement the 3 percent M&A allocation allowed on subgrants. However, no more than 5 percent of the total subaward may be expended by subgrantees on M&A costs.

### **D.8. Construction and Renovation**

Construction and renovation is not allowed under MMRS.

# **X. CITIZEN CORPS PROGRAM**



## X. CITIZEN CORPS PROGRAM

### A. Program Overview

The FY 2006 CCP funds will be used to support Citizen Corps Councils with efforts to engage citizens in all-hazards prevention, protection, response, and recovery. These efforts include planning and evaluation, public education and emergency communications, training, exercises, volunteer programs and activities to support emergency responders, surge capacity roles and responsibilities, and providing proper equipment to citizen volunteers. The FY 2006 Citizen Corps funds provide resources for States and local communities to:

- 1) bring together the appropriate leadership to form and sustain a Citizen Corps Council;
- 2) develop and implement a plan or amend existing plans to achieve widespread citizen preparedness and participation;
- 3) conduct public education and outreach;
- 4) ensure clear emergency communications with the public;
- 5) develop training programs for the public;
- 6) facilitate citizen participation in exercises;
- 7) implement volunteer programs and activities to support emergency responders;
- 8) involve citizens in surge capacity roles and responsibilities; and
- 9) conduct evaluations of programs and activities.

### B. CCP and the National Preparedness Goal

The American citizens are the ultimate stakeholders in the homeland security mission and must be an integral component of national preparedness efforts. As such, the general public is included in the vision statement of the Goal which notes that citizens must have:

- a clear understanding of national preparedness
- regular outreach and communication
- alerts, warnings, and crisis communication
- opportunities to be involved

Community Preparedness and Participation is identified as a common Target Capability in the TCL that cuts across all mission areas and capabilities. It describes both universal and threat-based levels of citizen preparedness, and a support level of citizen participation through year-round volunteer service and surge capacity roles and responsibilities. Additionally, other capabilities in the TCL specifically address roles for the

#### Target Capabilities

- Community Preparedness and Participation

#### Citizen Preparedness and Participation Cuts Across:

- *Planning*
- *Communications*
- *Risk Management*
- *Info Gathering and Recognition of Indicators*
- *Law Enforcement Investigation and Operations*
- *Intelligence Analysis and Production*
- *CBRNE Detection*
- *Information Sharing*
- *Critical Infrastructure Protection*
- *Food & Ag Safety & Defense*
- *On-Site Incident Management*
- *Emergency Operations Center Management*
- *Isolation & Quarantine*
- *Critical Resource Logistics & Distribution*
- *Urban Search & Rescue*
- *Emergency Public Information & Warning*
- *Responder Health & Safety*
- *Triage & Pre-Hospital Treatment*
- *Public Safety & Security Response*
- *Citizen Protection: Evacuation and/or In-Place Protection*
- *Volunteer Management & Donations*
- *Medical Surge*
- *Animal Health Emergency Support*
- *Medical Supplies Management & Distribution*
- *Environmental Health & Vector Control*
- *Mass Prophylaxis*
- *Explosive Device Response Ops*
- *Mass Care*
- *Firefighting Operations/Support*
- *Fatality Management*
- *WMD/HazMat Response & Decontamination*

public, including Volunteer Management and Donations and Citizen Protection, Evacuation, and/or, In-Place Protection.

## **C. Program Requirements**

Expenditures must advance the Citizen Corps mission to have everyone participate in hometown security through preparedness activities, training, and volunteer service. In addition to HSGP funding, State and local governments are encouraged to consider all sources of funding, to include private sector funding, to leverage existing materials, to pursue economies of scale and scope in pursuing this mission, and to make expenditures that benefit multiple programs.

### **C.1. State Responsibilities**

The SAA must coordinate all citizen education, communication, training, and participation activities funded with any source of HSGP funds with the State agency currently responsible for the administration of Citizen Corps. In addition, the State Citizen Corps POC should be included in reviewing and revising the State and Urban Area Homeland Security Strategies. A listing of current State Citizen Corps POC is available at <http://www.citizencorps.gov/councils/> by selecting “State Citizen Corps POC List” on the left-hand side. In turn, the SAA must be included on the State Citizen Corps Council.

State Citizen Corps points of contact must also continue to provide program management via the administrative section of the Citizen Corps website, <http://www.citizencorps.gov>, to include managing the approval process for local Citizen Corps Councils, managing administrative section passwords for local users, and managing subscribers and e-mails to subscribers.

### **C.2. Reporting Requirements**

In addition to the BSIR reporting requirements for CCP as a component of FY 2006 HSGP, States and communities are also expected to register and update information regarding their Citizen Corps Councils and programs/activities on the Citizen Corps website and on other relevant programmatic websites, including CERT, Fire Corps, Medical Reserve Corps (MRC), Neighborhood Watch/USAonWatch, and Volunteers in Police Service (VIPS).

## **D. Authorized Program Expenditures**

Consistent with SHSP, CCP funding may be used in any of following categories:

- Planning (to include evaluation, public education/outreach, and citizen participation in volunteer programs and activities).
- Equipment.
- Training.
- Exercises.
- Personnel.
- M&A costs associated with implementing and managing CCP.

Expenditures must advance the Citizen Corps mission to have everyone participate in hometown security through preparedness activities, training, exercise, and volunteer service and the mission of the Ready Campaign to educate and empower citizens to prepare for emergencies. Please refer to Appendix D for additional information on authorized and unauthorized expenditures.

### **D.1. Planning**

Allowable planning costs include the establishment of Citizen Corps Councils, to include planning and evaluation. Costs associated with activities to develop and implement a State, regional, local, or Tribal Citizen Corps all-hazards strategic plan to engage the full community in hometown security are allowable. Citizen Corps implementation plans are not required to be submitted to G&T, but rather are essential tools to guide new and existing Citizen Corps Councils in achieving their goals and objectives for the community. Examples include:

- Conduct or participate in community assessments of vulnerabilities, resource needs, and determine citizen involvement to meet the needs.
- Work with emergency management structures to design surge strategies using citizen volunteers.
- Demonstrate use of Citizen Corps Councils as a tool to encourage cooperation and collaboration among community leaders when developing plans and implementation strategies.
- Provide opportunities for citizen to train and exercise with emergency responders to test plans, operations, and to participate in lessons learned.

In addition, efforts to include public communication and citizen participation in jurisdiction plans, such as EOPs, and to have citizen advocates sit on existing advisory councils and task forces is encouraged.

It is also critical to evaluate the impact of Citizen Corps Councils and Citizen Corps programs on the community. Expenditures to evaluate Citizen Corps Council programs and activities is allowable, to include assessing the effectiveness in engaging citizens, the impact on the community safety and quality of life, and a cost/benefit analysis.

### ***Public Education/Outreach***

In order to have a prepared and protected community and Nation, citizens must be educated, practiced and trained on how to prepare for and respond to emergencies, including natural disasters and potential terrorist attacks. To meet this goal, Citizen Corps Councils, States, regions and localities, can conduct public education campaigns to promote individual, family and business emergency preparedness. Citizen Corps Councils may develop or reproduce public education and outreach materials to educate and engage the public; conduct outreach and hold community events; and develop alerts, warning, and communications systems to the public, to include tailored materials and communications to special needs populations. Some examples include:

- Conduct public education campaigns to include promoting the Ready Campaign’s preparedness message.
- Conduct education and awareness campaigns to inform the public about local alerts and warning and evacuation plans.
- Develop targeted outreach for all ages, ethnic and cultural groups, individuals with disabilities, and special needs populations.

Allowable expenditures include:

- Materials to support a public awareness campaign, media coverage, outreach activities, and public events, such as: public safety announcements; printed advertising; billboards; promotional flyers; booth displays; conference backdrops; podium signs; recognition pieces for Citizen Corps participants; informational buttons, pins, key chains, clothing, badges, and magnets; newsletters, posters, buck slips; and other materials that either educate the public, encourage the public to participate, or recognize and support Citizen Corps partners and participants. All materials must include the Citizen Corps logo or the Ready logo, tagline, and website at a minimum, and comply with logo standards (See [https://www.citizencorps.gov/pdf/logo\\_guide.pdf](https://www.citizencorps.gov/pdf/logo_guide.pdf)).
- Outreach activities to support a public education campaign or Citizen Corps Council including hosting and participating in public events; facilitating media coverage and establishing partnerships to spread the emergency preparedness message. These activities may include expenditures on items such as: booth displays; media materials; event backdrops or signs; promotional materials such as buttons, pins, key chains, clothing, badges, and magnets; and other materials and activities that educate the public about emergency preparedness and encourage the public to take steps to prepare or get involved in preparing their communities. All materials should include the Ready or Citizen Corps logos, taglines and websites whenever possible.

***Citizen Participation/Volunteer Programs***

One of the goals for Citizen Corps Councils is to provide volunteer service opportunities across all emergency prevention, preparedness and response disciplines, for community safety efforts, and for disaster relief. Citizen Corps funding may be used to establish or enhance volunteer program and volunteer recruitment efforts for Neighborhood Watch, CERT, VIPS, MRC and Fire Corps; for the Citizen Corps affiliate programs; for other homeland security efforts at the State and local level; for outreach and training activities; and to support the Citizen Corps Council. Some examples include:

- Implement Citizen Corps programs at the community level to support local emergency responders. These include: Community Emergency Response Teams (CERT); Medical Reserve Corps (MRCs), Neighborhood Watch, Volunteers in Police Service (VIPs), Fire Corps, and the Affiliate Programs.
- Include Citizen Corps assets as key components of State and local volunteer and donation management plans.

To assist local communities with engaging volunteers, Citizen Corps funds may be used for costs including but not limited to: 1) recruiting; 2) screening/assessing; 3) training; 4) retaining/motivating; 5) implementing and maintaining a system to track activities and participants (in compliance with applicable privacy laws); 6) recognizing; 7) evaluating volunteers; 8) the purchase of or subscription to identification/credentialing systems to support the tracking of volunteers.

**D.2. Organization**

Organization activities allowed under the CCP program are limited to the development and support of citizen surge capabilities.

**D.3. Equipment**

Equipment for citizen participants is critical. Allowable equipment costs include: equipment related to specific training or volunteer assignments and outfitting trainees and volunteers with program-related materials and equipment, e.g., issuing CERT kits, credentials/badges, and identifying clothing; and providing necessary equipment to citizen volunteers with a surge capacity role. The FY 2006 AEL is available in its entirety online through the RKB at <http://www.rkb.mipt.org> and the equipment categories are outlined in Table 12 below and Appendix D.

**Table 12 – CCP Allowable Equipment Categories**

Cat. #	Category Title	Cat. #	Category Title
[4]	Information Technology	[10]	Power Equipment
[5]	Cyber Security Enhancement Equipment	[11]	CBRNE Reference Materials
[9]	Medical Supplies and Limited Types of Pharmaceuticals	[21]	Other Authorized Equipment

**D.4. Training**

Training is a central component of the Citizen Corps mission and training funding by these grants can include all-hazards safety such as emergency preparedness; basic first aid; life saving skills; crime prevention and terrorism awareness; public health issues; mitigation/property damage prevention; safety in the home; CERT; search and rescue skills; principles of NIMS/ICS, community relations, volunteer management; any training necessary to participate in volunteer activities; any training necessary to fulfill surge capacity roles; or other training that promotes community safety.

Training should be delivered in venues throughout the community, to include schools, neighborhoods, places of worship, private sector, non-government organizations (NGO), and government locations with specific consideration to include all ages, ethnic and cultural groups, persons with disabilities, and special needs populations. Jurisdictions are also encouraged to incorporate non-traditional methodologies such as the Internet, distance learning, home study, and to leverage existing training provided via educational/professional facilities. Pilot courses

and innovative approaches to training citizens are encouraged.

Instruction for trainers and training to support the Citizen Corps Council members in their efforts to manage and coordinate the Citizen Corps mission is also an allowable use of the FY 2006 Citizen Corps funding.

Allowable costs include: 1) instructor preparation and delivery time (to include overtime costs); 2) hiring of full- or part-time staff or contractors/consultants to assist with conducting the training and/or managing the administrative aspects of conducting the training; 3) quality assurance and quality control of information; 4) creation and maintenance of a student database; 5) rental of training facilities; 6) printing course materials to include instructor guides, student manuals, brochures, certificates, handouts, newsletters and postage (although preference is for an electronic newsletter with email addresses as part of the database unless the individuals or areas to be served have limited access to electronic communications); 7) course materials specific to the subject matter, such as instructor guides, student manuals, bandages, gloves, fire extinguishers, and mannequins; and 8) outfitting trainees and volunteers with program-related materials and equipment, e.g., issuing CERT kits, credentials/badges, identifying clothing.

#### **D.5. Exercises**

Exercises specifically designed for or to include citizens are allowable activities and may include testing public warning systems, evacuation/shelter in-place capabilities, family/business preparedness, and participating in table-top or full scale emergency responder exercises at the local, State, or national level, to include TOPOFF. Examples of appropriate volunteer citizen support for emergency preparedness and response exercises include, but are not limited to: backfilling non-professional tasks for first responders deployed on exercise, administrative and logistical assistance with exercise planning and implementation; providing simulated victims, press, and members of the public; functioning in a range of surge capacity roles; and participating in the after-action review.

Allowable costs include the costs associated with design, development, and conduct of exercises specifically for citizens or to support the citizen component of emergency responder exercises, to include preparing and debriefing citizens regarding their role in the exercise. Exercises should ensure that citizens, including citizens with disabilities, participate in all phases of emergency responder exercises, to include planning, implementation and after-action review.

Exercises conducted with G&T support (grant funds or direct support) must be managed and executed in accordance with the HSEEP. The HSEEP Volumes contain guidance and recommendations for designing, developing, conducting, and evaluating exercises. HSEEP Volume IV provides sample exercise materials. All four volumes can be found at the HSEEP website (<http://hseep.dhs.gov>).

#### **D.6. Personnel**

Hiring, overtime, and backfill expenses are allowable only to perform programmatic activities deemed allowable under existing guidance. Supplanting, however, is not allowed.

Up to 15% of programmatic spending may be used to support the hiring of full or part-time personnel to conduct program activities that are allowable under the entire FY 2006 HSGP (i.e., planning, training program management, exercise program management, etc). Grantees may request that DHS issue a waiver to increase that ceiling. Waiver decisions are at the discretion of DHS and will be considered on a case-by-case basis. The ceiling on personnel costs does not apply to contractors, and is in addition to eligible M&A costs and eligible hiring of intelligence analysts. Grantees may hire staff only for program management functions not operational duties. Hiring planners, training program coordinators, exercise managers, and grant administrators fall within the scope of allowable program management functions. Grant funds may not be used to support the hiring of sworn public safety officers to fulfill traditional public safety duties.

#### **D.7. Management and Administration**

No greater than 5 percent of the CCP allocation may be used for M&A. Local jurisdiction subgrantees may retain and use up to 3 percent of their subaward from the State for local M&A purposes. States may pass through a portion of the State M&A allocation to local subgrantees in order to supplement the 3 percent M&A allocation allowed on subgrants. However, no more than 5 percent of the total subaward may be expended by subgrantees on M&A costs.

#### **D.8. Construction and Renovation**

Construction and renovation is not allowed under CCP.

**APPENDIX A:**

**SAMPLE AWARD  
PACKAGE**



## APPENDIX A – SAMPLE AWARD PACKAGE

### TAB 1: SAMPLE REVIEW OF AWARD

**Preparedness Directorate’s Office of Grants and Training  
Office of Grant Operations  
Post Award Instructions for Office of Grants and Training Awards**

#### **1. Review Award and Special Conditions Document.**

Carefully read the award and any special conditions or other attachments. There is an original plus one copy of the award page.

**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 - Office of Grants and Training 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 Preparedness Officer as noted in the award package.

#### **2. Read Guidelines.**

Become familiar with the OGO Financial Management Guide, which is available by contacting OGO at 1-866-9ASKOGO. New award recipients are automatically placed on a mailing list to receive future Guides and their change sets.

Up to 5 copies of the Guide may be ordered at no cost through: <http://puborder.ncjrs.org>

You may also order the Guide by calling 1-800-851-3420. Select #2 for publications, select #1 to speak with a publications specialist.

## **TAB 2: SAMPLE POST AWARD INSTRUCTION**

Preparedness Directorate's Office of Grants and Training  
Office of Grant Operations  
Office of the Comptroller

### **Post Award Instructions**

OGO will provide fiscal support and oversight of the G&T grant programs, while the OJP OC will continue to provide support for grant payments. The following is provided as a guide for the administration of awards from G&T. Forms and other documents illustrating each step are attached.

#### **Step 1. Review Award and Special Conditions.**

**If you agree** with the terms and conditions stated in the award, sign and date the award document and the last page of the Special Conditions, and return to OJP. Notify an G&T Preparedness Officer when Special Conditions have been met (refer to Step 1 attachment);

**If you do not agree** with the terms and conditions as written, contact an G&T Preparedness Officer.

#### **Step 2. Read Guidelines.**

Read and become familiar with the OGO Financial Management Guide and related material

#### **Step 3. Complete and Return Automated Clearing House (ACH) Form.**

The ACH Vendor/Miscellaneous Payment Enrollment Form (refer to Step 3 attachment) is used to arrange direct deposit of funds into the designated bank account.

#### **Step 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 G&T grants on the LOCES grant number listing as soon as the G&T 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.

#### **Step 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.

## **Step 6. Questions about your G&T 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](mailto: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](mailto:ask-ogo@dhs.gov).

**APPENDIX B:**

**INVESTMENT  
JUSTIFICATION**

## APPENDIX B – INVESTMENT JUSTIFICATION

### A. OVERVIEW

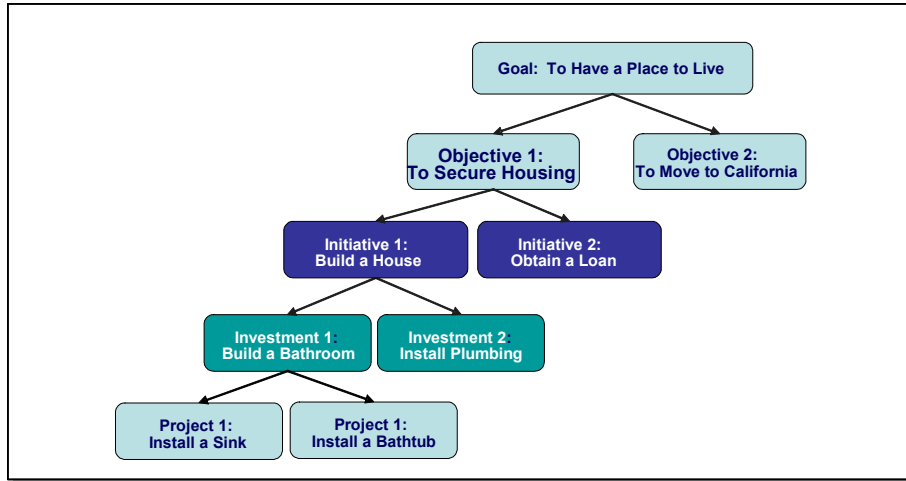
The Investment Justification is broken out into four (4) high-level sections. Each section has questions that must be completed. The high-level sections are: Background; Regionalization; Impact; and Funding and Implementation Plan. All questions in each section must be addressed in order for the Investment Justification to be considered complete. Additionally, an Investment Justification Summary Sheet will summarize the individual Investments and FY 2006 HSGP funding requests.

States and Urban Areas should develop an Investment Justification to request FY 2006 HSGP funding for those areas from the Enhancement Plan they have identified as priorities in the near-term. The application of FY 2006 HSGP funding towards the achievement of an Initiative(s) from the Enhancement Plan is called the *Investment*. States may propose up to 15 Investments for which they wish to utilize FY 2006 HSGP funds in the achievement and progress against the Initiatives from their Enhancement Plan. Additionally, Urban Areas may also propose up to 15 Investments, in addition to those proposed by the State. However, the Urban Area Investments must also support the achievement of an Initiative from their respective State's Enhancement Plan. Urban Area funding requests must be included as part of the State application submission. While States and Urban Areas will develop their own Investments, **the Urban Area Investment Justifications must be included as part of the overall State application submission.** States and Urban Areas are strongly encouraged to coordinate with each other to present an application that represents a collaborative, integrated approach, and to avoid duplication of efforts.

### B. CONTEXT

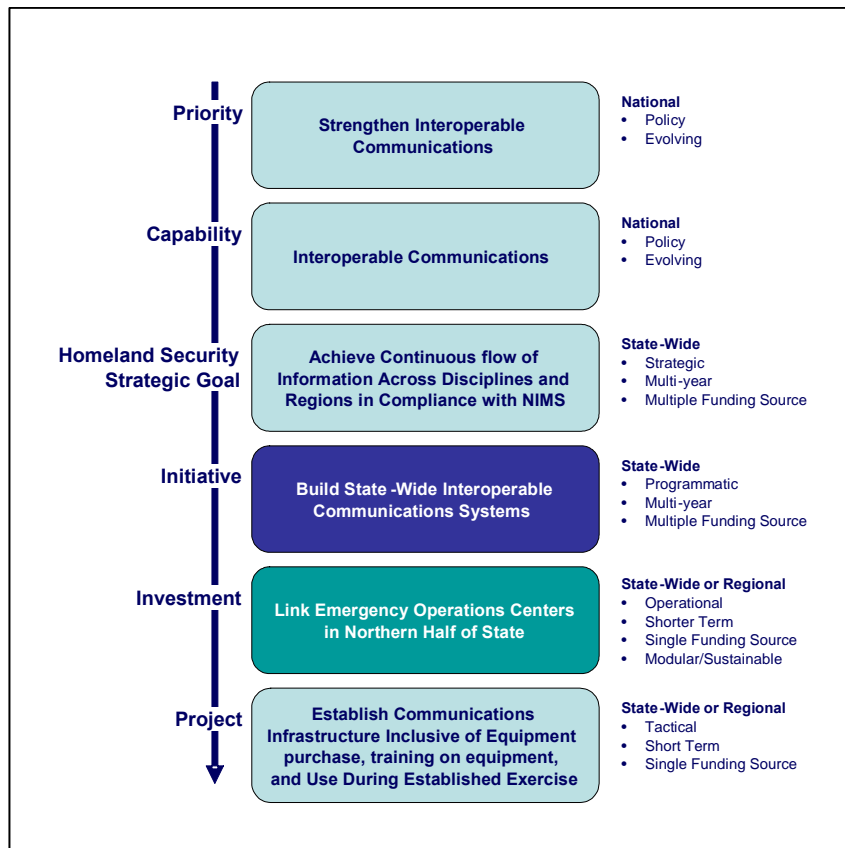
Investments proposed in the Investment Justification must relate directly to Initiatives in the Enhancement Plan, which in turn is related to the homeland security strategy goals and objectives. The following graphic provides an illustrative example of the relationship between Strategy goals and objectives, Enhancement Plan Initiatives, Investments, and projects:

**Figure 3 – Relationship of Initiatives to Goals, Objectives, Investments, and Projects**



The following graphic further illustrates the relationship of an Investment to the National Priorities, Target Capabilities:

**Figure 4 – Interoperable Communications as a Priority, Capability, Strategic Goal, Initiative and Investment, and Project**



### C. INVESTMENT JUSTIFICATION TEMPLATE

An Investment Justification template has been developed in Excel for use by the States and Urban Areas. This template will be provided to States and Urban Areas along with a users manual that will include instructions on how to complete the template itself, as well as guidance on the type of information to include in the responses to each question in the Investment Justification. States and Urban Areas are strongly encouraged to use the Excel template, as it will help ensure applications are complete and satisfy all requirements.

### D. INVESTMENT JUSTIFICATION QUESTIONS

Screen shots of the Investment Justification template in Excel are provided below. The screen shots are meant to provide the look and feel of how the template looks. **States and Urban areas should not use the screen shots that follow to complete their Investment Justification, and must use the template in Microsoft® Excel that will be provided.**

INVESTMENT #

1

State/Territory Name:

FY 2006 Urban Area Name:

Investment Name:

FY 2006 HSGP Funding Request:

I. BACKGROUND

I.A: Provide a summary description of this Investment and its purpose. (Not to exceed 200 words)

I.B: Explain how the Investment will support the implementation of an Initiative(s) from the Program and Capability Enhancement Plan, and the achievement of goals and objectives from your State/Urban Area homeland security strategy(ies). (Not to exceed 300 words)

I.C: List up to four National Priority(ies) this Investment primarily supports.

I.D: List up to six Target Capability(ies) from the Target Capabilities List this Investment primarily supports.

II. REGIONALIZATION

II.A: Describe the geographic and demographic area(s) this Investment covers. (Not to exceed 275 words)



INVESTMENT #

1

State/Territory Name:

FY 2006 HSGP Funding Request:

FY 2006 Urban Area Name:

Investment Name:

II.B: Explain how the State/Urban Area is organizing to implement this Investment over the identified geographic area(s).  
(Not to exceed 300 words)

II.C: Discuss the collaboration process you have, or will establish, with other regions and jurisdictions (inter- and intra-State) within or beyond the geographic/demographic area of this Investment. Discuss when and how you will engage stakeholders from those regions in specific support of this Investment. (Not to exceed 500 words)

SAMPLE

**III. IMPACT**

III.A: Discuss anticipated impacts of this Investment and how the requested funding will help attain/achieve expected impacts. Consider the population and areas affected, and other entities (jurisdictions, disciplines) that could leverage the outcomes and impacts of the solution presented by this Investment. (Not to exceed 500 words)

<b>INVESTMENT #</b>	State/Territory Name: <input style="width: 90%;" type="text"/>	FY 2006 HSGP Funding Request: <input style="width: 90%;" type="text"/>
<b>1</b>	FY 2006 Urban Area Name: <input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>
	Investment Name: <input style="width: 95%;" type="text"/>	

III.B: Discuss how the implementation of this Investment will decrease or mitigate risk. (Not to exceed 500 words)

III.C: Describe what the potential Homeland Security risks of not funding this Investment are. (Not to exceed 500 words)

SAMPLE

**IV. FUNDING & IMPLEMENTATION PLAN**

**IV.A: Investment Funding Plan**

	FY 2006 Homeland Security Grant Program Request					FY 2006 HSGP Request Total	Other Funding Sources Applied	Grand Total
	SHSP	UASI	LETPP	MMRS	CCP			
Personnel								
Planning								
Organization								
Equipment*								
Training								
Exercises								
M&A								
Total								

\*If you plan to purchase Interoperable Communications Equipment, your Investment Justification must include discussion on planning, governance, training, policies, procedures, and/or exercises related to the equipment.

INVESTMENT #

1

State/Territory Name:

FY 2006 HSGP Funding Request:

FY 2006 Urban Area Name:

Investment Name:

IV.B: Identify potential challenges to the effective implementation of this Investment (e.g., stakeholder buy-in, sustainability, aggressive timelines). (Not to exceed 300 words)

IV.C: Explain how the identified challenges will be addressed and mitigated. (Not to exceed 300 words)

IV.D: Describe the management team, including roles and responsibilities, that will be accountable for the oversight and implementation of this Investment, and the overall management approach they will apply for the implementation of this Investment. (Not to exceed 300 words)

SAMPLE

<b>INVESTMENT #</b>	State/Territory Name: <input style="width: 90%;" type="text"/>	FY 2006 HSGP Funding Request: <input style="width: 90%;" type="text"/>
<b>1</b>	FY 2006 Urban Area Name: <input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>
	Investment Name: <input style="width: 95%;" type="text"/>	

IV.E: Discuss funding resources beyond FY 2006 HSGP that have been identified and will be leveraged to support the implementation and sustainment of this Investment. (Not to exceed 300 words)

IV.F: Provide a high-level timeline, including milestones and dates, for the implementation of this Investment. Possible areas for inclusion are: stakeholder engagement, planning, major acquisitions/purchases, training, exercises, and process/policy updates. Space is provided for up to 10 milestones, but not all 10 spaces may be necessary for the response. ("Milestone" not to exceed 25 words and "Related Activities" not to exceed 100 words)

<b>Milestone #1</b>	<input style="width: 95%;" type="text"/>	Start Date: <input style="width: 80%;" type="text"/>	End Date: <input style="width: 80%;" type="text"/>
<b>Related Activities</b>	<input style="width: 95%;" type="text"/>		
<b>Milestone #2</b>	<input style="width: 95%;" type="text"/>	Start Date: <input style="width: 80%;" type="text"/>	End Date: <input style="width: 80%;" type="text"/>
<b>Related Activities</b>	<input style="width: 95%;" type="text"/>		
<b>Milestone #3</b>	<input style="width: 95%;" type="text"/>	Start Date: <input style="width: 80%;" type="text"/>	End Date: <input style="width: 80%;" type="text"/>
<b>Related Activities</b>	<input style="width: 95%;" type="text"/>		
<b>Milestone #4</b>	<input style="width: 95%;" type="text"/>	Start Date: <input style="width: 80%;" type="text"/>	End Date: <input style="width: 80%;" type="text"/>
<b>Related Activities</b>	<input style="width: 95%;" type="text"/>		
<b>Milestone #5</b>	<input style="width: 95%;" type="text"/>	Start Date: <input style="width: 80%;" type="text"/>	End Date: <input style="width: 80%;" type="text"/>
<b>Related Activities</b>	<input style="width: 95%;" type="text"/>		

<b>INVESTMENT #</b>	State/Territory Name: <input style="width: 90%;" type="text"/>	FY 2006 HSGP Funding Request: <input style="width: 90%;" type="text"/>
<b>1</b>	FY 2006 Urban Area Name: <input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>
	Investment Name: <input style="width: 95%;" type="text"/>	

<b>Milestone #6</b>	<input style="width: 95%;" type="text"/>	Start Date: <input style="width: 80%;" type="text"/>
		End Date: <input style="width: 80%;" type="text"/>
<b>Related Activities</b>	<input style="width: 95%;" type="text"/>	
<b>Milestone #7</b>	<input style="width: 95%;" type="text"/>	Start Date: <input style="width: 80%;" type="text"/>
		End Date: <input style="width: 80%;" type="text"/>
<b>Related Activities</b>	<input style="width: 95%;" type="text"/>	
<b>Milestone #8</b>	<input style="width: 95%;" type="text"/>	Start Date: <input style="width: 80%;" type="text"/>
		End Date: <input style="width: 80%;" type="text"/>
<b>Related Activities</b>	<input style="width: 95%;" type="text"/>	
<b>Milestone #9</b>	<input style="width: 95%;" type="text"/>	Start Date: <input style="width: 80%;" type="text"/>
		End Date: <input style="width: 80%;" type="text"/>
<b>Related Activities</b>	<input style="width: 95%;" type="text"/>	
<b>Milestone #10</b>	<input style="width: 95%;" type="text"/>	Start Date: <input style="width: 80%;" type="text"/>
		End Date: <input style="width: 80%;" type="text"/>
<b>Related Activities</b>	<input style="width: 95%;" type="text"/>	

**IV.G:** Describe the planned duration for this overall Investment. Discuss your long-term sustainability plans for the Investment after your FY 2006 HSGP funds have been expended, if applicable. (Not to exceed 300 words)

## **E. INVESTMENT JUSTIFICATION SUMMARY SHEET**

The Investment Justification template will include an Investment Justification Summary Sheet. The Summary Sheet will be entirely populated by information entered in the individual Investment Justification worksheets. States and Urban Areas should submit one summary sheet that will provide an overview for all Investments addressed in the Investment Justification. A screen shot of the Investment Justification Summary Sheet from the Excel template follows on the next page.

**Summary Sheet for FY 2006 HSGP Investment Justifications**

State/Territory Name:  Total FY 2006 HSGP Request:

FY 2006 Urban Area Name:

**INVESTMENT SUMMARY INFORMATION**

#	Investment Name	FY 2006 HSGP Request
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		

**STATE/TERRITORY-WIDE FUNDING PLAN SUMMARY FOR ALL INVESTMENTS**

	FY 2006 Homeland Security Grant Program Request					FY 2006 HSGP Request Total	Other Funding Sources Applied	Grand Total
	SHSP	UASI	LETPP	MMRS	CCP			
Personnel								
Planning								
Operations								
Equipment								
Training								
Exercises								
M&A								
Total								

**APPENDIX C:**

**MEMORANDUM OF  
UNDERSTANDING  
TEMPLATE**



## APPENDIX C – MEMORANDUM OF UNDERSTANDING TEMPLATE

### MEMORANDUM OF UNDERSTANDING / AGREEMENT BETWEEN THE STATE OF (STATE) AND THE (LOCAL GOVT TYPE) OF (LOCAL GOVT) REGARDING STATE USE OF HOMELAND SECURITY GRANT FUNDING ON BEHALF OF (LOCAL GOVT)

**1. PARTIES.** The parties to this Agreement are the State of (STATE) and the (LOCAL GOVT TYPE) of (LOCAL GOVT).

**2. AUTHORITY.** This Agreement is authorized under the provisions of [APPROPRIATE STATE LAW – PLEASE ATTACH A COPY].

**3. PURPOSE.** The purpose of this Agreement is to set forth terms by which (STATE) shall expend Homeland Security Grant Funding on behalf of (LOCAL GOVT). On (DATE), the United States Department of Homeland Security issued grant number (GRANT NUMBER) to (STATE). Under this grant, the (STATE) must allocate grant funding to (LOCAL GOVT). Under this grant, (LOCAL GOVT) may authorize (STATE) to make purchases on behalf of (LOCAL GOVT), provided that (LOCAL GOVT) and (STATE) enter into an Agreement on the matter.

#### **4. RESPONSIBILITIES:**

a. (STATE)

(1) (STATE) shall assign title in all purchases to (LOCAL GOVT)

(2) (LOCAL GOVT)

**5. POINTS OF CONTACT.** [Identify the POCs for the State and local governments; including addresses and phone numbers (fax number, e-mail, or internet addresses can also be included).]

**6. OTHER PROVISIONS.** Nothing in this Agreement is intended to conflict with current laws or regulations of (STATE) or (LOCAL GOVT). If a term of this agreement is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this agreement shall remain in full force and effect.

**7. EFFECTIVE DATE.** The terms of this agreement will become effective on (EFFECTIVE DATE).

**8. MODIFICATION.** This agreement may be modified upon the mutual written consent of the parties.

**9. TERMINATION.** The terms of this agreement, as modified with the consent of both parties, will remain in effect until [GRANT END DATE]. Either party upon [NUMBER] days written notice to the other party may terminate this agreement.

**APPROVED BY:**

\_\_\_\_\_

(Date)

\_\_\_\_\_

(Date)

**APPENDIX D:**

**ALLOWABLE COST  
MATRIX**

## APPENDIX D – ALLOWABLE COST MATRIX

Table 13 – FY 2006 Allowable Cost Matrix

Allowable Planning Costs	HSGP					Other G&T					HHS			
	SHSP	UASI	LETPP	MMRS	CCP	EMPG	Transit	Port	Bus	Rail	Firefighters	NBHP	BTCDP	PHEPCA
Public education & outreach	Y	Y	Y	Y	Y	Y	Y			Y	Y			Y
Develop and implement homeland security support programs and adopt ongoing DHS National Initiatives	Y	Y	Y	Y	Y	Y	Y			Y				Y
Develop and enhance plans and protocols	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y		Y
Develop or conduct assessments	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y
Establish, enhance, or evaluate Citizen Corps related volunteer programs	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y
Hiring of full- or part-time staff or contract/consultants to assist with planning activities (not for the purpose of hiring public safety personnel fulfilling traditional public safety duties)	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y
Conferences to facilitate planning activities	Y	Y	Y	Y	Y	Y	Y		Y	Y				Y
Materials required to conduct planning activities	Y	Y	Y	Y	Y	Y	Y			Y				Y
Travel/per diem related to planning activities	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y
Overtime and backfill costs (IAW operational Cost Guidance)	Y	Y	Y	Y	Y	Y	Y		Y	Y				
Other project areas with prior approval from G&T	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
Allowable Organizational Activities	SHSP	UASI	LETPP	MMRS	CCP	EMPG	Transit	Port	Bus	Rail	Firefighters	NBHP	BTCDP	PHEPCA
Overtime for information, investigative, and intelligence sharing activities (up to 25 percent of the allocation)		Y	Y											
Reimbursement for select operational expenses associated with increased security measures at critical infrastructure sites incurred during periods of DHS-declared Code Orange		Y	Y				Y							
Hiring of full- part-time staff or contractors for emergency management activities					Y	Y					Y			
Hiring of contractors/consultants for participation in information/intelligence analysis and sharing groups or fusion center activities (limited to 25 percent of the allocation)		Y	Y											

Allowable Equipment Categories	HSGP					Other G&T					HHS			
	SHSP	UASI	LETTP	MMRS	CCP	EMPG	Transit	Port	Bus	Rail	Firefighters	NBHPP	BTCDP	PHRPCA
Personal Protective Equipment	Y	Y	Y	Y			Y			Y	Y	Y		Y
Explosive Device Mitigation and Remediation Equipment	Y	Y	Y				Y	Y	Y	Y	Y			
CBRNE Operational Search and Rescue Equipment	Y	Y	Y	Y			Y	Y	Y	Y	Y			
Information Technology	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y
Cyber Security Enhancement Equipment	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
Interoperable Communications Equipment	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y		Y
Detection Equipment	Y	Y		Y		Y	Y	Y	Y	Y	Y			Y
Decontamination Equipment	Y	Y		Y			Y		Y	Y	Y	Y		Y
Medical Supplies and Limited Pharmaceuticals	Y	Y		Y	Y	Y	Y		Y	Y	Y	Y		
Power Equipment	Y	Y	Y	Y	Y		Y		Y	Y	Y			
CBRNE Reference Materials	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y
CBRNE Incident Response Vehicles	Y	Y	Y	Y		Y	Y		Y	Y	Y			
Terrorism Incident Prevention Equipment	Y	Y	Y				Y	Y	Y	Y	Y			
Physical Security Enhancement Equipment	Y	Y	Y			Y	Y	Y	Y	Y				
Inspection and Screening Systems	Y	Y	Y	Y			Y	Y			Y			
Agriculture Terrorism Prevention, Response and Mitigation Equipment	Y	Y		Y										
CBRNE Response Watercraft	Y	Y	Y				Y	Y	Y	Y				
CBRNE Aviation Equipment	Y	Y												
CBRNE Logistical Support Equipment	Y	Y	Y	Y		Y	Y		Y	Y	Y			
Intervention Equipment	Y	Y	Y				Y		Y	Y				
Other Authorized Equipment	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
Allowable Training Costs	SHSP	UASI	LETTP	MMRS	CCP	EMPG	Transit	Port	Bus	Rail	Firefighters	NBHPP	BTCDP	PHRPCA
Overtime and backfill for emergency preparedness and response personnel attending G&T-sponsored and approved training classes	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y			
Overtime and backfill expenses for part-time and volunteer emergency response personnel participating in G&T training	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y			
Training workshops and conferences	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y
Full- or part-time staff or contractors/consultants	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y
Travel	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y
Supplies	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y
Other items	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y			
Allowable Exercise Related Costs	SHSP	UASI	LETTP	MMRS	CCP	EMPG	Transit	Port	Bus	Rail	Firefighters	NBHPP	BTCDP	PHRPCA

	HSGP						Other G&T				HHS			
Exercise planning workshop	Y	Y	Y	Y	Y	Y	Y			Y				Y
Full- or part-time staff or contractors/consultants	Y	Y	Y	Y	Y	Y	Y			Y				Y
Overtime and backfill costs including expenses for part-time and volunteer emergency response personnel participating in G&T exercises	Y	Y	Y	Y	Y	Y	Y			Y				
Travel	Y	Y	Y	Y	Y	Y	Y			Y				Y
Supplies	Y	Y	Y	Y	Y	Y	Y			Y				Y
Other items	Y	Y	Y	Y	Y	Y	Y			Y				
<b>Allowable Management &amp; Administrative Costs</b>	<b>SHSP</b>	<b>UASI</b>	<b>LETPP</b>	<b>MMRS</b>	<b>CCP</b>	<b>EMPG</b>	<b>Transit</b>	<b>Port</b>	<b>Bus</b>	<b>Rail</b>	<b>Firefighters</b>	<b>NBHP</b>	<b>BTCDP</b>	<b>PHEPCA</b>
Hiring of full- or part-time staff or contractors/consultants to assist with the management of HSGP, implementation of State Homeland Security Strategy, application requirements, compliance with reporting and data collection requirements	Y	Y	Y	Y	Y	Y				Y	Y			Y
Development of operating plans for information collection and processing necessary to respond to G&T Data calls	Y	Y	Y	Y	Y	Y	Y		Y	Y				
Overtime and backfill costs	Y	Y	Y	Y	Y	Y								Y
Travel	Y	Y	Y	Y	Y	Y	Y		Y	Y				Y
Meeting related expenses	Y	Y	Y	Y	Y	Y	Y		Y	Y				Y
Authorized office equipment	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y			
Recurring expenses such as those associated with cell phones and faxes during the period of performance of the Grant Program	Y	Y	Y	Y	Y	Y					Y			Y
Leasing or renting of space for newly hired personnel during the period of performance of the Grant Program	Y	Y	Y	Y	Y	Y					Y			

Costs outlined in the following table are **NOT allowed** unless designated by a “\*”. Those designated by a “\*” are only allowable in a limited capacity. Check the specific program guidance for detailed information.

Unauthorized Program Expenditures	HSGP					Other G&T					HHS			
	SHSP	UASI	LETP	MMRS	CCP	EMPG	Transit	Port	Bus	Rail	Firefighters	NBHP	BTCDP	PHEPCA
General use software, computers and related equipment, vehicles, licensing fees						*	*				*	*	*	
Weapons and Ammunition														
Construction and Renovation ( <b>ONLY limited</b> renovation is allowable in highlighted programs)	*	*	*			*					*	*	*	*
Hiring of public safety personnel for the purpose of fulfilling traditional public safety duties						*					*	*	*	*
Activities unrelated to the completion and implementation of HSGP												*	*	
Other items not in accordance with the AEL or previously listed allowable costs												*	*	*

**APPENDIX E:**

**HISTORICAL  
ALLOWABLE DATA**



## APPENDIX E – HISTORICAL ALLOWABLE DATA

The following tables show how allowable costs have changed since FY 2003 for the various G&T grant programs under the categories of Planning, Equipment (AEL Categories), Training, Exercises, and Management and Administration.

**Table 14 – Historical Planning Categories**

Planning Costs	FY 2003				FY 2004				FY 2005				FY 2006						
	SHSGP	SHSGP II	UASI	UASI II	SHSP	LETPP	CCP	UASI	SHSP	UASI	LETPP	CCP	EMPG	MMRS	SHSP	UASI	LETPP	CCP	MMRS
Implementing and managing programs for equipment acquisition, training and exercises	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Develop and enhance plans and protocols	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Develop or conduct assessments	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Establish and/or enhance Citizen Corps Councils to include planning and evaluation	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Develop and implement homeland security support programs and adopt ongoing DHS national initiatives	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Materials and Meeting Related Expenses	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Hiring of full or part-time staff or contractors/consultants to assist with any related planning activities (not for the purpose of hiring public safety personnel)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

**Table 15 – Historical Equipment Costs**

Authorized Equipment List Categories	FY 2003				FY 2004				FY 2005				FY 2006						
	FY03 SHSGP	FY03 SHSGP II	FY03 UASI	FY03 UASI II	SHSP	LETPP	CCP	FY04 UASI	SHSP	UASI	LETPP	CCP	EMPG	MMRS	SHSP	UASI	LETPP	CCP	MMRS
1 Personal Protective Equipment	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y		Y
2 Explosive Device Mitigation and Remediation Equipment	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y				Y	Y	Y		
3 CBRNE Operational and Search & Rescue Equipment	Y	Y	Y	Y	Y			Y	Y	Y				Y	Y	Y	Y		Y
4 Information Technology								Y	Y	Y		Y		Y	Y	Y	Y	Y	Y
5 Cyber Security Enhancement Equipment					Y	Y		Y	Y	Y	Y			Y	Y	Y	Y	Y	Y
6 Interoperable Communications Equipment	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y			Y	Y	Y	Y		Y
7 Detection Equipment	Y	Y	Y	Y	Y			Y	Y	Y				Y	Y	Y			Y
8 Decontamination Equipment	Y	Y	Y	Y	Y			Y	Y	Y				Y	Y	Y			Y

		FY 2003			FY 2004			FY 2005					FY 2006							
Authorized Equipment List Categories		FY03 SHSGP	FY03 SHSGP II	FY03 UASI	FY03 UASI II	SHSP	LETPP	CCP	FY04 UASI	SHSP	UASI	LETPP	CCP	EMPG	MMRS	SHSP	UASI	LETPP	CCP	MMRS
		9	Medical Supplies and Limited Types of Pharmaceuticals	Y	Y	Y	Y	Y			Y	Y	Y				Y	Y	Y	
10	Power Equipment								Y	Y	Y				Y	Y	Y	Y	Y	Y
11	CBRNE Reference Materials	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
12	CBRNE Incident Response Vehicles	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y				Y	Y	Y		Y
13	Terrorism Incident Prevention Equipment	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y				Y	Y	Y		
14	Physical Security Enhancement Equipment	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y				Y	Y	Y		
15	Inspection and Screening Systems								Y	Y	Y					Y	Y	Y		Y
16	Agricultural Terrorism Prevention, Response and Mitigation Equipment					Y			Y	Y	Y					Y	Y			Y
17	CBRNE Prevention and Response Watercraft					Y	Y		Y	Y	Y	Y				Y	Y	Y		
18	CBRNE Aviation Equipment					Y			Y	Y	Y					Y	Y			
19	CBRNE Logistical Support Equipment	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y			Y	Y	Y	Y		Y
20	Intervention Equipment					Y	Y		Y	Y	Y	Y				Y	Y	Y		
21	Other Authorized Equipment					Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

**Table 16 – Historical Training Costs**

		FY 2003			FY 2004			FY 2005					FY 2006							
Training Costs		FY03 SHSGP	FY03 SHSGP II	FY03 UASI	FY03 UASI II	SHSP	LETPP	CCP	FY04 UASI	SHSP	UASI	LETPP	CCP	EMPG	MMRS	SHSP	UASI	LETPP	CCP	MMRS
			Establishment of CBRNE training capacities	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y		Y	Y			
	Training workshops and conferences					Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Overtime and backfill funding for emergency preparedness and response personnel attending G&T-sponsored and approved training classes		Y O/T only	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y
	Full or part-time staff or contractors/consultants					Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Creation and maintenance of student databases							Y												
	Travel			Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Supplies					Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

**Table 17 – Historical Exercise Costs**

Exercise Costs	FY 2003				FY 2004			FY 2005					FY 2006						
	FY03 SHSGP	FY03 SHSGP II	FY03 UASI	FY03 UASI II	SHSP	LETPP	CCP	FY04 UASI	SHSP	UASI	LETPP	CCP	EMPG	MMRS	SHSP	UASI	LETPP	CCP	MMRS
Design, development, conduct and evaluation of exercises	Y	Y	Y	Y	Y	Y	Y for citizens	Y	Y	Y	Y	Y for citizens	Y	Y					
Expenses related to Exercise Planning Workshops	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Costs Related to the Implementation of the HSEEP	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y					
Hiring of full or part-time staff or contractors/consultants	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Overtime	Y	Y	Y	Y	Y*	Y*	Y*	Y*	Y*	Y*	Y*	Y*	Y*	Y*	Y*	Y*	Y*	Y*	Y*
Travel	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Supplies	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

\* - denotes that “backfill” is also allowed.

**Table 18 – Historical Management & Administrative Costs**

Management & Administrative Costs	FY 2003				FY 2004			FY 2005					FY 2006						
	FY03 SHSGP	FY03 SHSGP II	FY03 UASI	FY03 UASI II	SHSP	LETPP	CCP	FY04 UASI	SHSP	UASI	LETPP	CCP	EMPG	MMRS	SHSP	UASI	LETPP	CCP	MMRS
Conduct training sessions ensure accurate completion of the needs assessment	Y	Y																	
Updating and refining Statewide Homeland Security Strategic plans	Y	Y																	
Conducting local or regional strategy implementation meetings	Y	Y	Y	Y															
Meeting-related expenses	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Development of operating plans for information collection and processing necessary to respond to G&T data calls									Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Implementing and managing programs for equipment acquisition, training and exercise	Y	Y																	

Management & Administrative Costs	FY 2003				FY 2004				FY 2005					FY 2006					
	FY03 SHSGP	FY03 SHSGP II	FY03 UASI	FY03 UASI II	SHSP	LETPP	CCP	FY04 UASI	SHSP	UASI	LETPP	CCP	EMPG	MMRS	SHSP	UASI	LETPP	CCP	MMRS
Hiring part-time staff or contractors/consultants to assist with management, implementation and administration	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Overtime and backfill									Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Travel	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Leasing and/or renting of office space for newly hired personnel					Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Recurring fees/charges associated with certain equipment, such as cell phones, faxes, etc. (allowable only within the period of performance of the grant program)					Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Acquisition of authorized office equipment (includes personal computers, laptops, printers, LCD projectors and other equipment or software which may be required to support implementation of the State strategy)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
The percentage of the program that may be used for M&A	3%	3%	3%	3%	3%	3%	3%	3%	3%	3%	3%	3%	3%	3%	5%	5%	5%	5%	5%
Percentage of grant program that may be subawarded from the State for local M&A purposes									3%	3%	3%	3%	3%	3%	3%	3%	3%	3%	3%
Pass-through Requirements	>= 80%	>= 80%	>= 80%	>= 80%	>= 80%	>= 80%	>= 80%	>= 80%	>= 80%	>= 80%	>= 80%	No Min	100 %	>= 80%	>= 80%	>= 80%	>= 80%	No Min	>= 80%

# **APPENDIX F:**

## **RELATIONSHIP OF GRANT PROGRAMS TO TARGET CAPABILITIES**

## APPENDIX F – RELATIONSHIP OF GRANT PROGRAMS TO TARGET CAPABILITIES

Grant programs link to the Target Capabilities according to the following table. “Y” denotes a direct role for the capability, while “\*” denotes a supporting role.

**Table 19 – Relationship of Grants to Target Capabilities**

37 Target Capabilities and Categories	SHSP	UASI	LETPP	MMRS	CCP	EMPG	Transit	Port	Bus	Rail	Firefighters	NBHP	BTCDP	PHEPCA
<b>Common Target Capabilities</b>														
Planning	Y	Y	Y	Y	*	Y	Y	Y	Y	Y	Y	Y		Y
Community Preparedness and Participation	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
Communications	Y	Y	Y	Y	*	Y	Y	Y	Y	Y	Y	Y		Y
Risk Management	Y	Y			*	Y	Y	Y	Y	Y				
<b>Prevent Mission Area Target Capabilities</b>														
Info Gathering and Recognition of Indicators and Warnings	Y	Y	Y	Y	*		Y	Y	Y	Y				
Law Enforcement Investigation and Operations	Y	Y	Y		*		Y	Y		Y				
Intelligence Analysis and Production	Y	Y	Y		*		Y	Y		Y				
CBRNE Detection	Y	Y	Y	Y	*	Y	Y	Y	Y	Y	Y	Y	Y	
Intelligence / Information Sharing and Dissemination	Y	Y	Y		*	Y	Y	Y	Y	Y				
<b>Protect Mission Area Target Capabilities</b>														
Critical Infrastructure Protection	Y	Y	Y		*		Y	Y	Y	Y				
Epidemiological Surveillance & Investigation	Y	Y		Y								Y	Y	Y
Public Health Laboratory Testing	Y	Y		Y								Y	Y	Y
Food and Agriculture Safety and Defense	Y	Y			*	Y								
<b>Respond Mission Area Target Capabilities</b>														
Onsite Incident Management	Y	Y			*	Y	Y	Y	Y	Y	Y	Y		
Citizen Protection: Evacuation and/or In-Place Protection	Y	Y		Y	*	Y	Y	Y	Y	Y				
Emergency Operations Center Management	Y	Y			*	Y	Y	Y	Y	Y				
Isolation and Quarantine	Y	Y		Y	*	Y	Y	Y		Y		Y		Y
Critical Resource Logistics and Distribution	Y	Y		Y	*	Y	Y	Y	Y	Y				
Urban Search & Rescue	Y	Y		Y	*	Y	Y			Y	Y			
Volunteer Management and Donations	Y	Y			*	Y								
Emergency Public Information and Warning	Y	Y		Y	*	Y	Y	Y	Y	Y				Y
Responder Safety and Health	Y	Y		Y	*	Y	Y	Y	Y	Y	Y	Y	Y	Y
Triage and Pre-Hospital Treatment	Y	Y		Y	*		Y	Y	Y	Y	Y	Y	Y	
Public Safety and Security Response	Y	Y		Y	*	Y	Y	Y	Y	Y	Y			
Medical Surge	Y	Y		Y	*							Y	Y	
Animal Health Emergency Support	Y	Y			*									Y
Medical Supplies Management and Distribution	Y	Y		Y	*	Y	Y	Y	Y	Y		Y	Y	
Environmental Health	Y	Y		Y	*									Y
Mass Prophylaxis	Y	Y		Y	*	Y	Y	Y	Y	Y		Y	Y	Y
Explosive Device Response Operations	Y	Y			*		Y	Y		Y	Y			
Mass Care	Y	Y		Y	*	Y	Y	Y	Y	Y				

<b>37 Target Capabilities and Categories</b>	<b>SHSP</b>	<b>UASI</b>	<b>LE/TPP</b>	<b>MMRS</b>	<b>CCP</b>	<b>EMPG</b>	<b>Transit</b>	<b>Port</b>	<b>Bus</b>	<b>Rail</b>	<b>Firefighters</b>	<b>NBHP</b>	<b>BTCDP</b>	<b>PHPCA</b>
Firefighting Operations/Support	Y	Y		Y	*		Y	Y	Y	Y	Y			
Fatality Management	Y	Y		Y	*	Y	Y	Y	Y	Y		Y		
WMD/Hazardous Materials Response and Decontamination	Y	Y		Y	*	Y	Y	Y	Y	Y	Y	Y	Y	
<b>Recover Mission Area Target Capabilities</b>														
Structural Damage and Mitigation Assessment	Y	Y			*		Y	Y	Y	Y				
Economic & Community Recovery	Y	Y			*	Y	Y	Y	Y	Y				
Restoration of Lifelines	Y	Y			*		Y	Y	Y	Y				

**APPENDIX G:**

**NIMS STATE,  
TERRITORIAL, AND  
TRIBAL COMPLIANCE  
ACTIVITIES**



## APPENDIX G – NIMS STATE, TERRITORIAL AND TRIBAL COMPLIANCE ACTIVITIES

### A. FY 2006 STATE AND TERRITORIAL COMPLIANCE ACTIVITIES

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 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<sup>1</sup> play an important 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<sup>2</sup> 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:

---

<sup>15</sup> As defined in the Homeland Security Act of 2002, the term “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.” 6 U.S.C. 101 (14)

<sup>2</sup> 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 U.S.C. 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).

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](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](http://www.fema.gov/nims).

In Federal 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](http://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 FY2006 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 FY2007 and beyond.

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

**Table 20 – NIMS Implementation Matrix for States and Territories**

<b>FY 2006 Compliance Activities</b>		
<b>Required State/Territorial Action for FY 2006 Compliance</b>	<b>Guidance and Technical Assistance Resources</b>	<b>Future Activities</b>
<b>State Adoption and Infrastructure</b>		
<p>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.</p> <p>Monitor formal adoption of NIMS by all Tribal and local jurisdictions.</p>	<ul style="list-style-type: none"> <li>• Adopt NIMS through executive order, proclamation, resolution or legislation as the State's official all-hazards, incident response system.</li> <li>• 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.</li> <li>• The NIMS Capability Assessment Support Tool (NIMCAST) is available at: <a href="http://www.fema.gov/nimcast/index.jsp">www.fema.gov/nimcast/index.jsp</a></li> <li>• Sample templates for executives: <a href="http://www.fema.gov/nims/nims_toolsandtemplates.shtm">www.fema.gov/nims/nims_toolsandtemplates.shtm</a></li> </ul>	<ul style="list-style-type: none"> <li>• Amend or re-authorize, as necessary.</li> </ul>
<p>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.</p>	<ul style="list-style-type: none"> <li>• FY 2006 NIMS Implementation Matrix for Local Jurisdictions</li> </ul>	
<p>Designate a single point of contact within the State government to serve as the principal coordinator for NIMS implementation Statewide.</p>	<ul style="list-style-type: none"> <li>• Consider establishing new or leverage existing cross-jurisdictional and cross-discipline advisory group to assist and ensure full implementation of NIMS.</li> </ul>	

FY 2006 Compliance Activities		
Required State/Territorial Action for FY 2006 Compliance	Guidance and Technical Assistance Resources	Future Activities
<p>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.</p>	<ul style="list-style-type: none"> <li>• The <i>National Incident Management System (NIMS)</i> March 2004, the NIMS implementation requirements, and Homeland Security Presidential Directive 5 are all available on the NIMS Web page at: <a href="http://www.fema.gov/nims">www.fema.gov/nims</a></li> <li>• NIMS Capability Assessment Support Tool (NIMCAST): <a href="http://www.fema.gov/nimcast/index.jsp">www.fema.gov/nimcast/index.jsp</a></li> <li>• 2005 Homeland Security Grant Program Guidance: <a href="http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf">http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf</a></li> <li>• National Preparedness Goal and National Preparedness Guidance: <a href="http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm">http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm</a></li> </ul>	
<p>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.</p>	<ul style="list-style-type: none"> <li>• The <i>National Incident Management System (NIMS)</i> March 2004, the NIMS implementation requirements, and Homeland Security Presidential Directive 5 are all available on the NIMS Web page at: <a href="http://www.fema.gov/nims">www.fema.gov/nims</a></li> <li>• NIMS Capability Assessment Support Tool (NIMCAST): <a href="http://www.fema.gov/nimcast/index.jsp">www.fema.gov/nimcast/index.jsp</a></li> <li>• A list of the Federal preparedness grant programs that have been reported to the NIC are available on the NIMS Web page at: <a href="http://www.fema.gov/nims">www.fema.gov/nims</a></li> <li>• 2005 Homeland Security Grant Program Guidance: <a href="http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf">http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf</a></li> <li>• National Preparedness Goal and National Preparedness Guidance: <a href="http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm">http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm</a></li> </ul>	
<b>Command and Management</b>		
<p><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.</p>	<ul style="list-style-type: none"> <li>• Institutionalize ICS: Terms and definitions: <a href="http://www.fema.gov/txt/nims/institutionalizing_ics.txt">www.fema.gov/txt/nims/institutionalizing_ics.txt</a></li> <li>• 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.</li> </ul>	<ul style="list-style-type: none"> <li>• Continue to manage incidents and events using ICS.</li> </ul>

**FY 2006 Compliance Activities**

<b>Required State/Territorial Action for FY 2006 Compliance</b>	<b>Guidance and Technical Assistance Resources</b>	<b>Future Activities</b>
<p><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.</p>	<ul style="list-style-type: none"> <li>• NIMS Chapter II, Command and Management.</li> </ul>	<ul style="list-style-type: none"> <li>• Revise and update processes and plans.</li> <li>• 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 <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> <li>• The NIMS Integration Center will feature best practices on the NIMS Web page. See <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> </ul>

## FY 2006 Compliance Activities

Required State/Territorial Action for FY 2006 Compliance	Guidance and Technical Assistance Resources	Future Activities
<p><u>Public Information System:</u></p> <p>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</p>	<ul style="list-style-type: none"> <li>• NIMS Chapter II, Command and Management.</li> <li>• Public Information Training (E388, Advanced Public Information Officers and G290, Basic Public Information Officers)</li> </ul>	<ul style="list-style-type: none"> <li>• Revise and update processes and plans.</li> <li>• 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 <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> <li>• Information on who should complete these courses also will be posted on the NIMS Web page.</li> <li>• The NIMS Integration Center will feature best practices on the NIMS Web page. See <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> </ul>
<b>Preparedness: Planning</b>		
<p>Establish the State's NIMS baseline against the FY 2005 and FY 2006 implementation requirements</p>	<ul style="list-style-type: none"> <li>• Assess which NIMS implementation requirements the State already meets. The NIMS Capability Assessment Support Tool (NIMCAST) is available to facilitate this: <a href="http://www.fema.gov/nimcast/index.jsp">www.fema.gov/nimcast/index.jsp</a></li> </ul>	<ul style="list-style-type: none"> <li>• Update State's Homeland Security strategy and any other State preparedness strategies and plans as appropriate and close capability gap.</li> </ul>
<p>Coordinate and leverage all Federal preparedness funding to implement the NIMS.</p>	<ul style="list-style-type: none"> <li>• A list of the Federal preparedness grant programs that have been reported to the NIC are available on the NIMS Web page at: <a href="http://www.fema.gov/nims">www.fema.gov/nims</a></li> <li>• 2005 Homeland Security Grant Program Guidance: <a href="http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf">http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf</a></li> <li>• National Preparedness Goal and National Preparedness Guidance: <a href="http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm">http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm</a></li> <li>• Catalog of Federal Domestic Preparedness Assistance (CFDA): <a href="http://www.cfda.gov">http://www.cfda.gov</a></li> </ul>	

FY 2006 Compliance Activities		
Required State/Territorial Action for FY 2006 Compliance	Guidance and Technical Assistance Resources	Future Activities
<p>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</p>	<ul style="list-style-type: none"> <li>• National Response Plan (NRP): <a href="http://www.dhs.gov/nationalresponseplan">http://www.dhs.gov/nationalresponseplan</a></li> <li>• 2005 Homeland Security Grant Program Guidance: <a href="http://www.ojp.usdoj.gov/odp/docs/fy05hsgrp.pdf">http://www.ojp.usdoj.gov/odp/docs/fy05hsgrp.pdf</a></li> <li>• National Preparedness Goal and National Preparedness Guidance: <a href="http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm">http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm</a></li> </ul>	<ul style="list-style-type: none"> <li>• Update plans and SOPs, incorporating lessons learned and best practices from exercises and response operations.</li> <li>• Emergency Operations Plan (EOP) guidance is under development and will be posted on the NIMS Integration Center Web page at: <a href="http://www.fema.gov/nims">www.fema.gov/nims</a>.</li> </ul>
<p>Promote intrastate and interagency mutual aid agreements, to include agreements with the private sector and non-governmental organizations.</p>	<ul style="list-style-type: none"> <li>• EMAC model State-county mutual aid deployment contract: <a href="http://www.emacweb.org/?123">http://www.emacweb.org/?123</a></li> <li>• EMAC model intrastate mutual aid legislation: <a href="http://www.emacweb.org/docs/NEMA%20Proposed%20Intrastate%20Model-Final.pdf">http://www.emacweb.org/docs/NEMA%20Proposed%20Intrastate%20Model-Final.pdf</a></li> </ul>	<ul style="list-style-type: none"> <li>• Expand mutual aid agreements beyond support services and equipment to include information sharing.</li> <li>• Support and adopt the ongoing efforts of the NIMS Integration Center (NIC) to develop a national credentialing system.</li> <li>• 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.</li> <li>• Credential first responders in conformance with national standards.</li> </ul>
<b>Preparedness: Training</b>		
<p>Leverage training facilities to coordinate and deliver NIMS training requirements in conformance with the NIMS National Standard Curriculum.</p>	<ul style="list-style-type: none"> <li>• NIMS National Standard Curriculum Training Development Guidance: <a href="http://www.fema.gov/pdf/nims/nims_training_development.pdf">http://www.fema.gov/pdf/nims/nims_training_development.pdf</a></li> </ul>	



## 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	<ul style="list-style-type: none"> <li>• On-line course: <a href="http://training.fema.gov/EMIWeb/IS/is700.asp">http://training.fema.gov/EMIWeb/IS/is700.asp</a></li> <li>• NIMS National Standard Curriculum Training Development Guidance: <a href="http://www.fema.gov/pdf/nims/nims_training_development.pdf">http://www.fema.gov/pdf/nims/nims_training_development.pdf</a></li> <li>• All personnel with a direct role in emergency preparedness, incident management or response must complete this training.</li> </ul>	<ul style="list-style-type: none"> <li>• Ensure that NIMS is part of the program for all new employees, recruits and first responders.</li> <li>• 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 <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> </ul>
Complete IS-800 NRP: An Introduction	<ul style="list-style-type: none"> <li>• On-line course available at: <a href="http://www.training.fema.gov/emiweb/IS/is800.asp">http://www.training.fema.gov/emiweb/IS/is800.asp</a></li> <li>• NIMS National Standard Curriculum Training Development Guidance: <a href="http://www.fema.gov/pdf/nims/nims_training_development.pdf">http://www.fema.gov/pdf/nims/nims_training_development.pdf</a></li> <li>• The NIMS Web page provides guidance for who should complete this training. <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> </ul>	<ul style="list-style-type: none"> <li>• Ensure that NRP training is part of the program for all appropriate employees, recruits and first responders.</li> <li>• 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 <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> </ul>

## 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	<ul style="list-style-type: none"> <li>• ICS 100: <a href="http://www.training.fema.gov/emiweb/IS/is100.asp">http://www.training.fema.gov/emiweb/IS/is100.asp</a></li> <li>• ICS 100: <a href="http://www.usfa.fema.gov/training/nfa">http://www.usfa.fema.gov/training/nfa</a></li> <li>• ICS 200: <a href="http://www.training.fema.gov/emiweb/IS/is200.asp">http://www.training.fema.gov/emiweb/IS/is200.asp</a></li> <li>• ICS 200: <a href="http://www.usfa.fema.gov/training/nfa">http://www.usfa.fema.gov/training/nfa</a></li> <li>• NIMS National Standard Curriculum Training Development Guidance: <a href="http://www.fema.gov/pdf/nims/nims_training_development.pdf">http://www.fema.gov/pdf/nims/nims_training_development.pdf</a></li> <li>• The NIMS Web page provides guidance for who should complete this training. <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> </ul>	<ul style="list-style-type: none"> <li>• Complete ICS 300 and ICS 400.</li> <li>• Complete training that may be required to satisfy credentialing standards.</li> <li>• Ensure that ICS training is part of the program for all new employees, recruits and first responders.</li> </ul>
<b>Preparedness: Exercises</b>		
Incorporate NIMS/ICS into all State and regional training and exercises.	<ul style="list-style-type: none"> <li>• NIMS training information: <a href="http://www.fema.gov/nims/nims_training.shtm">www.fema.gov/nims/nims_training.shtm</a></li> <li>• NIMS National Standard Curriculum Training Development Guidance: <a href="http://www.fema.gov/pdf/nims/nims_training_development.pdf">http://www.fema.gov/pdf/nims/nims_training_development.pdf</a></li> <li>• DHS G&amp;T Exercise Information: <a href="http://www.ojp.usdoj.gov/odp/exercises.htm">http://www.ojp.usdoj.gov/odp/exercises.htm</a></li> </ul>	<ul style="list-style-type: none"> <li>• Continue to incorporate NIMS into all State training and exercises, to include drills, tabletop exercises, functional exercises and full-scale exercises.</li> </ul>
Participate in an all-hazard exercise program based on NIMS that involves responders from multiple disciplines and multiple jurisdictions.	<ul style="list-style-type: none"> <li>• 2005 Homeland Security Grant Program Guidance: <a href="http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf">http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf</a></li> <li>• National Preparedness Goal and National Preparedness Guidance: <a href="http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm">http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm</a></li> <li>• DHS G&amp;T Exercise Information: <a href="http://www.ojp.usdoj.gov/odp/exercises.htm">http://www.ojp.usdoj.gov/odp/exercises.htm</a></li> <li>• NIMS National Standard Curriculum Training Development Guidance: <a href="http://www.fema.gov/pdf/nims/nims_training_development.pdf">http://www.fema.gov/pdf/nims/nims_training_development.pdf</a></li> </ul>	<ul style="list-style-type: none"> <li>• Continue to participate in NIMS -oriented exercises, to include drills, tabletop exercises, functional exercises and full-scale exercises.</li> </ul>
Incorporate corrective actions into preparedness and response plans and procedures.	<ul style="list-style-type: none"> <li>• DHS G&amp;T Exercise Information: <a href="http://www.ojp.usdoj.gov/odp/exercises.htm">http://www.ojp.usdoj.gov/odp/exercises.htm</a></li> </ul>	

FY 2006 Compliance Activities		
Required State/Territorial Action for FY 2006 Compliance	Guidance and Technical Assistance Resources	Future Activities
<b>Resource Management</b>		
Inventory State response assets to conform to homeland security resource typing standards.	<ul style="list-style-type: none"> <li>Resource typing definitions: <a href="http://www.fema.gov/nims/mutual_aid.shtm">http://www.fema.gov/nims/mutual_aid.shtm</a></li> <li>Propose modifications or new resource definitions to the NIMS Integration Center for inclusion in the resource typing effort.</li> </ul>	<ul style="list-style-type: none"> <li>Develop and implement a resource inventory, ordering and tracking system.</li> <li>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 <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a> when the course is available.</li> </ul>
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	<ul style="list-style-type: none"> <li><a href="http://www.dhs.gov/nationalresponseplan">http://www.dhs.gov/nationalresponseplan</a></li> </ul>	
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.	<ul style="list-style-type: none"> <li>G&amp;T Equipment Program: <a href="http://www.ojp.usdoj.gov/odp/grants_goals.htm">http://www.ojp.usdoj.gov/odp/grants_goals.htm</a></li> <li>2005 Homeland Security Grant Program Guidance: <a href="http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf">http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf</a></li> <li>National Preparedness Goal and National Preparedness Guidance: <a href="http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm">http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm</a></li> <li>DHS SAFECOM Program: <a href="http://www.safecomprogram.gov/SAFECOM">http://www.safecomprogram.gov/SAFECOM</a></li> </ul>	

FY 2006 Compliance Activities		
Required State/Territorial Action for FY 2006 Compliance	Guidance and Technical Assistance Resources	Future Activities
<b>Communication &amp; Information Management</b>		
<p>Apply standardized and consistent terminology, including the establishment of plain English communications standards across public safety sector.</p>	<ul style="list-style-type: none"> <li>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.</li> <li>'10' codes may continue to be used during non-emergency, internal Department communications.</li> </ul>	<ul style="list-style-type: none"> <li>Continue featuring common terminology and plain English commands for all response activities.</li> <li>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 <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> <li>Information on who should complete these courses also will be posted on the NIMS Web page.</li> </ul>

## B. FY 2006 TRIBAL GOVERNMENT AND LOCAL JURISDICTION COMPLIANCE ACTIVITIES

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<sup>1</sup> and local<sup>2</sup> 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:

---

<sup>16</sup> As defined in the Homeland Security Act of 2002, the term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States." 6 U.S.C. 101 (14)

<sup>2</sup> 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 U.S.C. 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; and
- 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](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 attached 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 FY2007 and beyond.

More 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>).

**Table 21 – NIMS Implementation Matrix for Tribal and Local Jurisdictions**

Required Tribal/Local Jurisdiction Action for FY 2006 Compliance	FY 2006 Compliance Activities	
	Guidance and Technical Assistance Resources	Future Activities
<b>Community Adoption</b>		
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.	<ul style="list-style-type: none"> <li>• Adopt NIMS through executive order, proclamation, resolution, or legislation as the jurisdiction's official all-hazards, incident response system.</li> <li>• 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.</li> <li>• The NIMS Capability Assessment Support Tool (NIMCAST) is available at: <a href="http://www.fema.gov/nimcast/index.jsp">www.fema.gov/nimcast/index.jsp</a></li> <li>• Sample templates for executives: <a href="http://www.fema.gov/nims/nims_toolsandtemplates.shtm">www.fema.gov/nims/nims_toolsandtemplates.shtm</a></li> </ul>	<ul style="list-style-type: none"> <li>• Amend or re-authorize, as necessary.</li> </ul>
<b>Command and Management</b>		

FY 2006 Compliance Activities		
Required Tribal/Local Jurisdiction Action for FY 2006 Compliance	Guidance and Technical Assistance Resources	Future Activities
<p><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.</p>	<ul style="list-style-type: none"> <li>• Institutionalize ICS: Terms and definitions: <a href="http://www.fema.gov/txt/nims/institutionalizing_ics.txt">www.fema.gov/txt/nims/institutionalizing_ics.txt</a></li> <li>• 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.</li> </ul>	<ul style="list-style-type: none"> <li>• Continue to manage incidents and events using ICS.</li> </ul>
<p><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 (ICPs, local 911 Centers, local Emergency Operations Centers (EOCs) and State EOC.</p>	<ul style="list-style-type: none"> <li>• NIMS Chapter II, Command and Management.</li> </ul>	<ul style="list-style-type: none"> <li>• Revise and update processes and plans.</li> <li>• 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 <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> <li>• The NIMS Integration Center will feature best practices on the NIMS Web page. See <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> </ul>



FY 2006 Compliance Activities		
Required Tribal/Local Jurisdiction Action for FY 2006 Compliance	Guidance and Technical Assistance Resources	Future Activities
<p><u>Public Information System:</u> 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.</p>	<ul style="list-style-type: none"> <li>• NIMS Chapter II, Command and Management.</li> <li>• Public Information Training (E388, Advanced Public Information Officers and G290, Basic Public Information Officers)</li> </ul>	<ul style="list-style-type: none"> <li>• Revise and update processes and plans.</li> <li>• 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 <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> <li>• Information on who should complete these courses also will be posted on the NIMS Web page.</li> <li>• The NIMS Integration Center will feature best practices on the NIMS Web page. See <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> </ul>
<b>Preparedness: Planning</b>		
<p>Establish the community's NIMS baseline against the FY 2005 and FY 2006 implementation requirements.</p>	<ul style="list-style-type: none"> <li>• Assess which NIMS implementation requirements your community already meets. The NIMS Capability Assessment Support Tool (NIMCAST) is available to facilitate this: <a href="http://www.fema.gov/nimcast/index.jsp">www.fema.gov/nimcast/index.jsp</a></li> </ul>	<ul style="list-style-type: none"> <li>• Update strategy as appropriate and close capability gap.</li> </ul>
<p>Develop and implement a system to coordinate all Federal preparedness funding to implement the NIMS across the community.</p>	<ul style="list-style-type: none"> <li>• A list of the Federal preparedness grant programs that have been reported to the NIC are available on the NIMS Web page at: <a href="http://www.fema.gov/nims">www.fema.gov/nims</a></li> <li>• 2005 Homeland Security Grant Program Guidance: <a href="http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf">http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf</a></li> <li>• National Preparedness Goal and National Preparedness Guidance:  <a href="http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm">http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm</a></li> <li>• Catalog of Federal Domestic Preparedness Assistance (CFDA): <a href="http://www.cfda.gov">http://www.cfda.gov</a></li> </ul>	

FY 2006 Compliance Activities		
Required Tribal/Local Jurisdiction Action for FY 2006 Compliance	Guidance and Technical Assistance Resources	Future Activities
<p>Revise and update plans and SOPs to incorporate NIMS components, principles and policies, to include planning, training, response, exercises, equipment, evaluation, and corrective actions</p>	<ul style="list-style-type: none"> <li>2005 Homeland Security Grant Program Guidance: <a href="http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf">http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf</a></li> <li>National Preparedness Goal and National Preparedness Guidance: <a href="http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm">http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm</a></li> </ul>	<ul style="list-style-type: none"> <li>Update plans and SOPs, incorporating lessons learned and best practices from exercises and response operations.</li> <li>Emergency Operations Plan (EOP) guidance is under development and will be posted on the NIMS Integration Center Web page at: <a href="http://www.fema.gov/nims">www.fema.gov/nims</a>.</li> </ul>
<p>Participate in and promote intrastate and interagency mutual aid agreements, to include agreements with the private sector and non-governmental organizations.</p>	<ul style="list-style-type: none"> <li>EMAC model State-county mutual aid deployment contract: <a href="http://www.emacweb.org/?123">http://www.emacweb.org/?123</a></li> <li>EMAC model intrastate mutual aid legislation: <a href="http://www.emacweb.org/docs/NEMA%20Proposed%20Intrastate%20Model-Final.pdf">http://www.emacweb.org/docs/NEMA%20Proposed%20Intrastate%20Model-Final.pdf</a></li> </ul>	<ul style="list-style-type: none"> <li>Expand mutual aid agreements beyond support services and equipment to include information sharing.</li> <li>Support and adopt the ongoing efforts of the NIMS Integration Center (NIC) to develop a national credentialing system.</li> <li>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.</li> <li>Credential first responders in conformance with national standards.</li> </ul>
<b>Preparedness: Training</b>		
<p>Complete IS-700 NIMS: An Introduction</p>	<ul style="list-style-type: none"> <li>On-line course: <a href="http://training.fema.gov/EMIWeb/IS/is700.asp">http://training.fema.gov/EMIWeb/IS/is700.asp</a></li> <li>NIMS National Standard Curriculum Training Development Guidance: <a href="http://www.fema.gov/pdf/nims/nims_training_development.pdf">http://www.fema.gov/pdf/nims/nims_training_development.pdf</a></li> <li>All personnel with a direct role in emergency preparedness, incident management, or response must complete this training</li> </ul>	<ul style="list-style-type: none"> <li>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.</li> <li>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 <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> </ul>

<b>FY 2006 Compliance Activities</b>		
<b>Required Tribal/Local Jurisdiction Action for FY 2006 Compliance</b>	<b>Guidance and Technical Assistance Resources</b>	<b>Future Activities</b>
Complete IS-800 NRP: An Introduction	<ul style="list-style-type: none"> <li>On-line course available at: <a href="http://www.training.fema.gov/emiweb/IS/is800.asp">http://www.training.fema.gov/emiweb/IS/is800.asp</a></li> <li>NIMS National Standard Curriculum Training Development Guidance: <a href="http://www.fema.gov/pdf/nims/nims_training_development.pdf">http://www.fema.gov/pdf/nims/nims_training_development.pdf</a></li> <li>The NIMS Web page provides for who should complete this training. <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a></li> </ul>	<ul style="list-style-type: none"> <li>Ensure that NRP training is part of the program for all appropriate new employees, recruits and first responders.</li> <li>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 <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> </ul>
Complete ICS 100 and ICS 200 Training	<ul style="list-style-type: none"> <li>ICS 100: <a href="http://www.training.fema.gov/emiweb/IS/is100.asp">http://www.training.fema.gov/emiweb/IS/is100.asp</a></li> <li>ICS 100: <a href="http://www.usfa.fema.gov/training/nfa">http://www.usfa.fema.gov/training/nfa</a></li> <li>ICS 200: <a href="http://www.training.fema.gov/emiweb/IS/is200.asp">http://www.training.fema.gov/emiweb/IS/is200.asp</a></li> <li>ICS 200: <a href="http://www.usfa.fema.gov/training/nfa">http://www.usfa.fema.gov/training/nfa</a></li> <li>NIMS National Standard Curriculum Training Development Guidance: <a href="http://www.fema.gov/pdf/nims/nims_training_development.pdf">http://www.fema.gov/pdf/nims/nims_training_development.pdf</a></li> <li>The NIMS Web page provides guidance for who should complete this training. <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> </ul>	<ul style="list-style-type: none"> <li>Complete ICS 300 and ICS 400.</li> <li>Complete training that may be required to satisfy credentialing standards.</li> <li>Ensure that ICS training is part of the program for all new employees, recruits and first responders.</li> <li>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 <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>.</li> </ul>
<b>Preparedness: Exercises</b>		
Incorporate NIMS/ICS into all Tribal, local and regional training and exercises.	<ul style="list-style-type: none"> <li>NIMS training information: <a href="http://www.fema.gov/nims/nims_training.shtm">www.fema.gov/nims/nims_training.shtm</a></li> <li>NIMS National Standard Curriculum Training Development Guidance: <a href="http://www.fema.gov/pdf/nims/nims_training_development.pdf">http://www.fema.gov/pdf/nims/nims_training_development.pdf</a></li> <li>DHS G&amp;T Exercise Information: <a href="http://www.ojp.usdoj.gov/odp/exercises.htm">http://www.ojp.usdoj.gov/odp/exercises.htm</a></li> </ul>	<ul style="list-style-type: none"> <li>Continue to incorporate NIMS into all local training and exercises, to include drills, tabletop exercises, functional exercises, and full-scale exercises.</li> </ul>

<b>FY 2006 Compliance Activities</b>		
<b>Required Tribal/Local Jurisdiction Action for FY 2006 Compliance</b>	<b>Guidance and Technical Assistance Resources</b>	<b>Future Activities</b>
Participate in an all-hazard exercise program based on NIMS that involves responders from multiple disciplines and multiple jurisdictions.	<ul style="list-style-type: none"> <li>• 2005 Homeland Security Grant Program Guidance: <a href="http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf">http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf</a></li> <li>• National Preparedness Goal and National Preparedness Guidance:  <a href="http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm">http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm</a></li> <li>• DHS G&amp;T Exercise Information: <a href="http://www.ojp.usdoj.gov/odp/exercises.htm">http://www.ojp.usdoj.gov/odp/exercises.htm</a></li> <li>• NIMS National Standard Curriculum Training Development Guidance: <a href="http://www.fema.gov/pdf/nims/nims_training_development.pdf">http://www.fema.gov/pdf/nims/nims_training_development.pdf</a></li> </ul>	<ul style="list-style-type: none"> <li>• Continue to participate in NIMS -oriented exercises, to include drills, tabletop exercises, functional exercises, and full-scale exercises.</li> </ul>
Incorporate corrective actions into preparedness and response plans and procedures.	<ul style="list-style-type: none"> <li>• DHS G&amp;T Exercise Information: <a href="http://www.ojp.usdoj.gov/odp/exercises.htm">http://www.ojp.usdoj.gov/odp/exercises.htm</a></li> </ul>	
<b>Resource Management</b>		
Inventory community response assets to conform to homeland security resource typing standards.	<ul style="list-style-type: none"> <li>• Propose modifications or new resource definitions to the NIMS Integration Center for inclusion in the resource typing effort.</li> <li>• Resource typing definitions: <a href="http://www.fema.gov/nims/mutual_aid.shtm">http://www.fema.gov/nims/mutual_aid.shtm</a></li> </ul>	<ul style="list-style-type: none"> <li>• Develop and implement a resource inventory, ordering, and tracking system.</li> <li>• 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 <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a> when the course is available.</li> </ul>

<b>FY 2006 Compliance Activities</b>		
<b>Required Tribal/Local Jurisdiction Action for FY 2006 Compliance</b>	<b>Guidance and Technical Assistance Resources</b>	<b>Future Activities</b>
<p>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.</p>	<ul style="list-style-type: none"> <li>• G&amp;T Equipment Program: <a href="http://www.ojp.usdoj.gov/odp/grants_goals.htm">http://www.ojp.usdoj.gov/odp/grants_goals.htm</a></li> <li>• 2005 Homeland Security Grant Program Guidance: <a href="http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf">http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf</a></li> <li>• National Preparedness Goal and National Preparedness Guidance: <a href="http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm">http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm</a></li> <li>• DHS SAFECOM Program: <a href="http://www.safecomprogram.gov/SAFECOM">http://www.safecomprogram.gov/SAFECOM</a></li> </ul>	
<b>Communication &amp; Information Management</b>		
<p>Apply standardized and consistent terminology, including the establishment of plain English communications standards across public safety sector.</p>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• '10' codes may continue to be used during non-emergency, internal Department communications.</li> </ul>	<ul style="list-style-type: none"> <li>• Continue featuring common terminology and plain English commands for all response activities.</li> <li>• 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 <a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a> when the course is available.</li> </ul>

**APPENDIX H:**  
**GEOSPATIAL GUIDANCE**

## APPENDIX H – GEOSPATIAL GUIDANCE

G&T recognizes the important contribution that geospatial information and technology plays in strengthening our Nation’s security posture. Federal, State and local organizations have increasingly incorporated geospatial information and technologies as tools for use in emergency management and homeland security applications. Geospatial data and systems improve the overall capability and information technology applications and systems to enhance public security and emergency preparedness and efficient response to all-hazards including both natural and man-made disasters.

DHS maintains a Geospatial Profile of the Homeland Security Enterprise Architecture and is working towards a National Strategy for a Homeland Security Geospatial Infrastructure. The purpose of these efforts are to help guide geospatial data and technology investments for building a standardized national model that will promote geospatial collaboration and interoperability among Homeland Security participants.

Grantees are recommended to review the guidance provided below. This will ensure that grantees have applied due diligence in reviewing and assessing requirements for their objectives that involve geospatial components.

### A. Considerations

The following considerations should be made when developing a geospatial program:

#### Coordination and Strategic Planning Considerations

- Does the State have a homeland security geospatial strategy or, at a minimum, address how geospatial data and technologies can support the State Homeland Security Strategy? Examples of strategies with geospatial content can be found on RKB, <http://www.rkb.mipt.org>.
- Has the State/jurisdiction identified homeland security geospatial requirements?
- Does the State have a geospatial coordination council that interfaces and coordinates with private, academic, military, and Tribal communities, and government agencies on homeland security geospatial information issues?
- Does the State/jurisdiction place an emphasis on making data readily available to other local jurisdictions, within their States, and with Federal agencies? Does the State/jurisdiction have data sharing agreements in place to support the homeland security mission? Does the State/jurisdiction include parcel information in these data sharing agreements?

#### Operational Considerations

- Does the State maintain a current inventory of geospatial assets (equipment, personnel, databases, services, metadata, systems, and documentation)?
- Does the State have homeland security geospatial data stored in more than one location and readily accessible to responders and to emergency operations centers?
- Does the State have access to a team of established geospatial personnel that can provide 24/7 expertise and equipment for emergencies?

- Does the State incorporate the use of geospatial applications into standard operating procedures for homeland security mission areas?
- Does the State have education and training programs for the use of geospatial applications in homeland security missions?

### **Compliance with Standards / Use of Best Practices Considerations**

- Does the State promote interoperability and efficient use of the geospatial data and services by complying with Federally-adopted geospatial standards, specifications, and guidelines such as those published by the Federal Geographic Data Committee (FGDC), the Open Geospatial Consortium (OGC™), the American National Standards Institute (ANSI), and the International Standards Organization (ISO)?
- Does the State register and/or publish the geospatial resources that are planned or result from programs or projects as a means to avoid expenditures of time, effort, and funds on redundant acquisitions?
- Does the State implement efficient geospatial metadata management capability following international and Federal Geographic Data Committee standards?
- Does the State/jurisdiction provide their geospatially related lessons learned via the Lessons Learned Information Sharing portal ([www.llis.gov](http://www.llis.gov))?

## **B. Recommended Content**

### **Minimum Essential Data Sets (MEDS)**

Federal, State, local, and Tribal governments worked together to create Minimum Essential Data Sets (MEDS) over urbanized areas as part of the Nunn-Lugar-Domenici 120-city effort, and for national critical infrastructure to fulfill the Joint Forces Command Common Relevant Operating Picture. Both sets of MEDS provide the geospatial foundation necessary for the Homeland Security Community to carry out the key national homeland security strategy objectives, as outlined by the White House on 16 July 2002 – (1) preventing terrorist attacks within the United States; (2) reducing the Nation’s vulnerability to terrorism; and (3) minimizing damage, while speeding recovery from natural or terrorist-caused disasters.

The Information Content Subgroup of the FGDC Homeland Security Working Group (HSWG) developed Guidelines for Homeland Security Infrastructure Protection Geospatial Data Content in October, 2005. This guidance is based on previous work done by members of the FGDC HSWG. The HSWG has improved the data content by: 1) refining feature and attribute requirements based on input from homeland security sector experts; 2) revising features, feature classes and definitions to correspond more closely with infrastructure data requirements of the DHS; and 3) indicating general priorities for feature and attribute collection. At the time of this publication, the geospatial content guidance is For Official Use Only (FOUO) and can be obtained by sending a request to the DHS Geospatial Management Office at [gmo@dhs.gov](mailto:gmo@dhs.gov). The e-mail should contain the requestor's name, organization, and description of need for this document.



### Data Quality

Two types of geographic areas are of special interest. For Urban Areas, the data should have the currency and positional accuracy qualities typically sought by local governments. For large areas (for example, States or groups of States), the data should have the positional accuracy qualities of USGS primary topographic map series (typically 1:24,000-scale; 1:63,360-scale in Alaska). Table 22 provides minimum goals for these two classes of data.

**Table 22 – Minimum (“no worse than”) Goals for Resolution, Accuracy, and Currency**

Data Theme	Urban Areas		Large Areas	
	Minimum Resolution or Accuracy <sup>17</sup>	Minimum Currency <sup>18</sup>	Minimum Resolution or Accuracy <sup>19</sup>	Minimum Currency
Orthoimagery	1 foot resolution; 3 meters horizontal accuracy	Two years	1 meter resolution; 11.70 meters horizontal accuracy	Five years
Elevation	1/9 arcsecond (~3 meters) resolution; 0.73 meter vertical accuracy	Two years	1/3 arcsecond (~10 meters) (2 arcsecond in Alaska) resolution; vertical accuracy commensurate with contour interval of USGS primary topographic map for area	Five years
Hydrography	4.68 meters horizontal accuracy	Two years	13.90 meters horizontal accuracy; 36.69 meters horizontal accuracy for Alaska	Five years
Transportation	4.68 meters horizontal accuracy	Two years	13.90 meters horizontal accuracy; 36.69 meters horizontal accuracy for Alaska	Five years
Boundaries	4.68 meters horizontal accuracy	Two years	13.90 meters horizontal accuracy; 36.69 meters horizontal accuracy for Alaska	Five years
Structures	4.68 meters horizontal accuracy	Two years	13.90 meters horizontal accuracy; 36.69 meters horizontal accuracy for Alaska	Five years
Land Cover	Should align with base maps that have the accuracies listed above.	Two years	Should align with base maps that have the accuracies listed above.	Five years
Geographic Names	Same as the associated feature		Same as the associated feature	

### C. Relevant Organizations and Initiatives

The following describes important organizations and those Federally-maintained, endorsed or adopted initiatives that grantees are strongly recommended to review:

<sup>17,4</sup> Accuracy statement based on Geospatial Positioning Accuracy Standard, Part 3, National Standard for Spatial Data Accuracy (FGDC-STD-007.3-1998). [http://www.fgdc.gov/standards/status/sub1\\_3.html](http://www.fgdc.gov/standards/status/sub1_3.html). For horizontal accuracies (95% confidence level), 3 meters is commensurate with 1:3,075-scale maps under the National Map Accuracy Standard, 4.68 meters with 1:4,800-scale maps, 13.90 meters with 1:24,000-scale maps, and 36.69 meters with 1:63,360-scale maps. For vertical accuracy (95% confidence level), 0.73 meter is commensurate with a four-foot contour interval under the National Map Accuracy Standard.

<sup>18,5</sup> Estimated currency of the data at the date of service initiation; that is, the data served reflects the ground condition sometime during the two (or five) years prior to the start of service through *The National Map*. (Note that, for themes in which the ground changes rarely, older data might meet this condition.)

<sup>19</sup> Data should be in the North American Datum of 1983; elevation data in the North American Vertical Datum of 1988.

**Federal Geographic Data Committee ([www.fgdc.gov](http://www.fgdc.gov))**

The FGDC is a 19-member interagency committee composed of representatives from the Executive Office of the President, Cabinet-level and independent agencies. The FGDC is developing NSDI in cooperation with organizations from State, local and Tribal governments, the academic community, and the private sector. NSDI encompasses policies, standards, and procedures for organizations to cooperatively produce and share geographic data.

**FGDC Metadata ([www.fgdc.gov/metadata/metadata.html](http://www.fgdc.gov/metadata/metadata.html))**

Metadata or "data about data" describe the content, quality, condition, and other characteristics of data. FGDC approved the Content Standard for Digital Geospatial Metadata (FGDC-STD-001-1998) in June 1998.

**FGDC Standards ([www.fgdc.gov/standards/standards.html](http://www.fgdc.gov/standards/standards.html))**

Standards facilitate the development, sharing, and use of geospatial data. The FGDC develops geospatial data standards for implementing the NSDI, in consultation and cooperation with State, local, and Tribal governments, the private sector and academic community, and, to the extent feasible, the international community.

**FGDC Framework ([www.fgdc.gov/framework/framework.html](http://www.fgdc.gov/framework/framework.html))**

GIS applications of many different disciplines have a recurring need for a few themes of data. The framework is a collaborative community based effort in which these commonly needed data themes are developed, maintained, and integrated by public and private organizations within a geographic area. Local, regional, State and Federal government organizations and private companies see the framework as a way to share resources, improve communications, and increase efficiency.

**Open Geospatial Consortium ([www.opengeospatial.org](http://www.opengeospatial.org))**

The Open Geospatial Consortium, Inc. (OGC™) is a nonprofit, international, voluntary consensus standards organization that is leading the development of standards for geospatial and location based services. Through member-driven consensus programs, OGC works with government, private industry, and academia to create open and extensible software application programming interfaces for geographic information systems and other mainstream technologies.

Consulting with the OGC specifications and standards is highly recommended for grantees interested in open, interoperable solutions; especially those involving publishing geospatial data and resources as a service. Many of the specifications, documents, and guidance provided here have been adopted as industry standard. Others are fairly new and not mature. Grantees are encouraged to comply with these consensual guidance and standards wherever relevant to specific projects and objectives.

To facilitate data discovery and sharing with other organizations, Web Map Service (WMS), Web Feature Service (WFS) and Geography Markup Language (GML) should be comply with OpenGIS interoperability specifications.

**National Spatial Data Infrastructure (NSDI) (<http://www.fgdc.gov/nsdi/nsdi.html>)**

The NSDI was created under Executive Order 12906 calling for the establishment of the

NSDI defined as the technologies, policies, and people necessary to promote sharing of geospatial data throughout all levels of government, private and nonprofit sectors, and the academic community.

The NSDI clearinghouse is available to Federal, State, local, and Tribal contributors to register as clearinghouse nodes where metadata about geospatial data, services, and resources can be published and harvested for discovery by any user. FGDC manages NSDI and provides guidance and instruction for using and registering nodes on NSDI.

States are encouraged to utilize Statewide coordinating councils to develop and maintain strategic and business plans for efficient Statewide geospatial data infrastructures in support of the National Spatial Data Infrastructure. DHS is encouraging States to examine Statewide or large regional approaches to the production of certain data, particularly framework (base map) data and critical infrastructure data that are conducive to Statewide data maintenance. Adopting this approach will align with Presidential directive A-16 for the National Spatial Data Infrastructure, save money, and promote data integration for mutual aid response.

Metadata of an organization's geographic data holdings is an important first step to participating in the NSDI. Metadata provides not only a way to inventory and preserve investments in costly geospatial data resources within an organization, but also is a means for its discovery and sharing with other organizations. Metadata standards recommended to comply include FGDC Content Standard for Digital Geospatial Metadata, Version 2 (CSDGM), FGDC-STD-001-1998 or when available the ISO Metadata Standard 19115 using draft ISO Technical Specification 19139; and Metadata Service Guidelines: Metadata must be posted and harvestable through the Geospatial One-Stop Portal at <http://www.GeoData.gov>.

#### **Geospatial One Stop Portal ([www.geodata.gov](http://www.geodata.gov))**

As a part of one of Office of Management and Budget's 24 Federal E-Gov initiatives ([www.whitehouse.gov/omb/egov/](http://www.whitehouse.gov/omb/egov/)), the Geospatial One Stop portal was established to promote data sharing across Federal entities and is available to the public for use as a discovery portal. Geospatial One Stop portal ([www.geodata.gov](http://www.geodata.gov)) is an interface to NSDI established under Executive Order 12906. The portal harvests geospatial resource metadata from nodes registered with NSDI and is a repository for all metadata published and accessible on NSDI. Users also have the option to publish metadata holdings directly to Geospatial One Stop enabling smaller organizations with the ability to share and collaborate on geospatial resources. Version 2 of the portal will be OGC standards enabled for OGC Web Map Service (WMS), Web Feature Service (WFS), and Catalog Service for the Web (CSW).

An important feature on Geospatial One Stop for grantees is the [geodata.gov](http://www.geodata.gov) Market Place. Here users can find information about planned acquisitions of geospatial resources and future projects or activities that may align with their own objectives. If grantees find no existing resources on Geospatial One Stop in either the metadata searches or in the Market Place, they are strongly encouraged to register their planned activities for geospatial data acquisition or future projects and activities so that others may prevent from redundant efforts.

### **The National Map (<http://nationalmap.gov/>)**

The U.S. Geological Survey (USGS) holds responsibility for maintaining nationally consistent foundation data layers that will support the DHS GEA. These data layers include:

- High-resolution digital orthorectified imagery from aerial photographs or satellite imagery.
- High-resolution surface elevation data to derive contours and digital terrain models.
- Vector feature data for hydrography (linear and open water bodies), transportation (roads, railway, and waterways), manmade structures, and boundaries.
- Land Cover that classifies land surface types.
- Geographic names of physical and cultural features (to support U.S. Board of Geographic Names).

Through partnerships that include cooperative arrangements for exchange of data, standards development, database development, web mapping services and applications, training, and technology exchange, the USGS has established a network of National Geospatial Partnership Offices and State Liaison positions across the Nation (<http://nationalmap.usgs.gov/partnerships.html>).

### **Ramona GIS Inventory (<http://www.gisinventory.net>)**

Ramona is a GIS inventory tool designed to work in concert with the Geospatial One Stop Portal. Ramona is produced by the National States' Geographic Information Council (NSGIC) as a tool for States and their partners. Its primary purpose is to track the status of GIS in US State and local government to aid the planning and building of Spatial Data Infrastructures.

### **U.S Army Corps of Engineers CADD/GIS Technology Center Spatial Data Standards (<http://tsc.wes.army.mil/products/TSSDS-TSFMS/tssds/html/>)**

The Spatial Data Standard for Facilities, Infrastructure, and Environment (SDSFIE) have focused on the development of graphic and non-graphic standards for GIS implementations at Air Force, Army, Navy, and Marine Corps installations, U.S. Army Corps of Engineers Civil Works activities, and other Government organizations.

The SDSFIE provides a standardized grouping of geographically referenced (i.e., geospatial) features (i.e., real-world features or objects depicted graphically on a map at their real-world location (i.e., coordinates). Each geospatial feature has an "attached" attribute table containing pertinent data about the geospatial feature.

### **American National Standards Institute (ANSI) INCITS Technical Committee L1**

(Geographic Information Systems ([http://www.ncits.org/tc\\_home/l1.htm](http://www.ncits.org/tc_home/l1.htm) and [http://www.ncits.org/stds\\_info.htm](http://www.ncits.org/stds_info.htm)))

International Committee for Information Technology Standards (INCITS) is the primary U.S. focus of standardization in the field of Information and Communications Technologies (ICT), encompassing storage, processing, transfer, display, management, organization, and retrieval of information. The work of INCITS Technical Committee L1, consists of adopting, adapting or developing information technology standards for use with digital geographic data. INCITS L1

serves as ANSI's U.S. Technical Advisory Group to the International Organization for Standardization (ISO) on matters concerning digital geographic information.

**United States National Grid** (<http://www.fgdc.gov/standards/status/usng.html>)

The objective of this U.S. National Grid standard is to create a more interoperable environment for developing location-based services within the United States and to increase the interoperability of location services appliances with printed map products by establishing a nationally consistent grid reference system as the preferred grid for NSDI applications. The U.S. National Grid is based on universally defined coordinate and grid systems and can, therefore, be easily extended for use world-wide as a universal grid reference system.

There are a number of coordinate reference systems that can be used either in location service appliances or on printed maps for the purpose of establishing a location. Within automated location service appliances, the conversion of coordinates based on one well-defined reference system to coordinates based on another can be both automatic and transparent to the user. These devices can support multiple coordinate reference systems with little difficulty. However, it is not easy for humans to work in multiple reference systems and humans cannot convert between systems without the aid of location service appliances, calculators, or conversion tables (FGDC-STD-011-2001).

**APPENDIX I:**

**CYBER SECURITY  
GUIDANCE**

## APPENDIX I – CYBER SECURITY GUIDANCE

Government entities at every level must have appropriate policies in place, understand where vulnerabilities exist, weigh the risks involved and make informed decisions on how to spend resources to secure data. Some 10,000 new computer viruses were reported last year, and it now only takes a few minutes to compromise an unprotected computer that is connected to the Internet. The negative impact of a virus or successful cyber attack can be devastating on networks, on the information contained within systems and, just as importantly, on the confidence of those who trust that government is working to increase protection.

Each State and local government entity should develop and execute a comprehensive cyber security plan that demonstrates due diligence in cyber security. The plan must account for factors such as limited staff and resources (and staff turnover); varying size and complexity of the State and local government entities; varying cyber security and technology knowledge base within government; and a wide variance in technology being used. In addition to a comprehensive plan, government must periodically test and exercise this plan, using vulnerability assessments to identify gaps and training needs.

All jurisdictions should ensure that their cyber security plan addresses four main areas: Policy, Training, Technology Deployment, and Vulnerability Assessment. Each of these areas supports the others, and together they meet emerging standards of due diligence in information security. The questions below are designed to identify key issues within each major area at the State level.

### Policy:

- Does the State have a cyber security plan in place that sets the vision, goals, and objectives for Statewide cyber security?
- Has the State published a clear policy statement on cyber security to support the plan, including “permitted use” policy for all State-owned cyber assets? Has this policy set been made available to jurisdictions within the State so that it can be adapted for their user?
- Has the State established a certification/accreditation program for information systems?
- Does the State have a designated cyber security office/officer whose primary focus is on protecting the State’s cyber infrastructure?
- Does the State have established cyber security metrics? Does the State have a mechanism for rating its cyber security alert level?
- Does the State maintain a current inventory of cyber assets, including personnel?
- Has the State established public, private, or academic partnerships for cyber security collaboration?
- Does the State have a capability for internal secure information sharing (Statewide secure portal)?
- Does the State have a formal mechanism for information sharing with external partners (including local government)?
- Does the State have a cyber operational center that functions 24/7? Does the State have an ad-hoc 24/7 capability if an operational center does not exist?
- Does the State have a Statewide Computer Security Incident Response Team?

- Does the State have a response plan for responding to critical cyber related events?
- Does this plan include a continuity of communications component?
- Does the State maintain a relationship with Federal entities such as the United States Computer Readiness Response Team (US-CERT)?

### **Training:**

- Are there requirements by the State to ensure employees have cyber security training and awareness on an annual basis?
- Are training programs available at multiple levels commensurate with employees' responsibility (e.g., general awareness, system administrator, network administrator)?
- Does the State have an outreach program to ensure the greatest penetration possible for cyber security awareness throughout State and local governments?
- Does the State have a web presence that provides cyber security guidance?
- Does the State have a program to establish and maintain a set of best practices for cyber security, both for its own use and to share with local jurisdictions?

### **Technology Deployment:**

- Has the State deployed appropriate technology for basic cyber security requirements such as anti-virus protection and network intrusion detection?
- Has the State deployed specific technology (including modifications and patches to existing systems and software) to respond to vulnerabilities identified by internal or third-party vulnerability assessments?
- Does the State have a system in place for tracking software versions in use, relevant known vulnerabilities, and available patches to counter those vulnerabilities.
- Does the State have cyber forensics capabilities to serve both civilian and criminal matters for the State?

### **Vulnerability Assessment:**

- Does the State have a formal program for periodic internal vulnerability assessment?
- Does the State supplement its internal assessment program with third-party vulnerability assessments?
- Is there a formal process by which assessment results are converted into prioritized remedial actions and tracked to completion?

Local jurisdictions should review many of the same questions, scaled to their individual needs. *Every government entity that owns and operates information technology equipment should have at least a rudimentary cyber security plan, and establish an Information Security Officer (ISO) or single point of contact (POC) for cyber security, including up-to-date 24/7 contact information.* Smaller jurisdictions should rely on their parent entities to provide sample policy documents and plans, as well as specialized assistance such as forensic analysis.

Grantees are urged to review the information at the following site, which provide valuable advice, best practices, and opportunities for support and information sharing:



**National Institute of Standards and Technology (NIST)**

<http://csrc.nist.gov/>

Founded in 1901, NIST is a non-regulatory Federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. The NIST Information Technology Laboratory, Computer Security Division provides a variety of tips, newsletters, and publications to support cyber security efforts.

**Multi-State Information Sharing and Analysis Center (MS-ISAC)**

<http://www.cscic.state.ny.us/msisac/index.html>

A public site identifying what the MS-ISAC is and what its mission, goals and objectives are in improving the Nation's cyber security posture from a State and local perspective. The goal is to have this MS-ISAC include all fifty States, which would provide a valuable centrally-coordinated mechanism for sharing important security intelligence and information between the States. The MS-ISAC can serve as a critical point of contact between the States and the Federal government. A primary goal of the MS-ISAC is to eliminate duplicative efforts.

**U.S. Computer Emergency Readiness Team (US CERT)**

<http://www.us-cert.gov/>

Established in 2003 to protect the Nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the Nation.

**The SANS™ Institute**

<http://www.sans.org>

SANS is an example of non-government cyber security resources, and is one of the largest sources for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and operates the Internet's early warning system - Internet Storm Center. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs who share the lessons they are learning and jointly find solutions to the challenges they face.

**National Strategy to Secure Cyberspace**

<http://www.whitehouse.gov/pcipb/>

The National Strategy to Secure Cyberspace is part of our overall effort to protect the Nation. It is an implementing component of the national Strategy for Homeland Security and is complemented by a national Strategy for the Physical Protection of Critical Infrastructures and Key Assets. The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact.

**APPENDIX J:**

**DOMESTIC NUCLEAR  
DETECTION OFFICE**

## **APPENDIX J – DOMESTIC NUCLEAR DETECTION OFFICE (DNDO)**

### **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. Federal, State, and Local 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 State and local entities that are involved in RAD/NUC preventive detection activities, DNDO is developing a database of State and local agencies 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 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, Polyvinyl Toluene (PVT) and spectroscopic, handheld and other mobile nuclear detection devices as well as radiography systems.

Funding from the SHSP, UASI, LETPP, BZPP, Transit Security Program, PSG, and IBSG Programs 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](mailto: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 TA programs for the enhancement and development of RAD/NUC preventive detection programs that support the planning, organization, equipment, training, and exercises activities (POETE model). This POETE framework matches to the Goal, State Homeland Security Strategies, 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 State and local agencies’ procurement decisions. Additionally, in FY 2006 DNDO anticipates developing guidance for establishing response protocols; guidance on linking programs to State fusion centers; and guidance on utilizing operational support systems. Table 23 provides an overview of the types of guidance and support systems that DNDO will develop.

**Table 23 – TA for RAD/NUC Preventive Detection Programs**

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

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

**APPENDIX K:**

**PUBLIC SAFETY  
COMMUNICATIONS &  
INTEROPERABILITY  
GUIDANCE**

## APPENDIX K – PUBLIC SAFETY COMMUNICATIONS & INTEROPERABILITY GUIDANCE

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, Federal FY 2006 Appropriations make available grant funding 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, 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 Department of Homeland Security’s National Incident Management System (NIMS).

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 ANSI/TIA/EIAA-102 Phase 1 (Project 25 or 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 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 Project 25 suite of standards for their new radio equipment. P25 has also been endorsed by the US Department of Defense for Private Wireless (PW—formerly called Land Mobile Radio) radio 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-Project 25 equipment when there are compelling reasons for using other solutions. Absent these compelling reasons, SAFECOM intends that Project 25 equipment will be preferred for digital systems to which the standard applies.

The SAFECOM grant guidance materials are available in their entirety on the SAFECOM website (<http://www.safecomprogram.gov>) in the electronic library. (See [http://www.safecomprogram.gov/SAFECOM/library/grant/1016\\_safecomgrant.htm](http://www.safecomprogram.gov/SAFECOM/library/grant/1016_safecomgrant.htm)).

**APPENDIX L:**  
**WEB RESOURCES**



## APPENDIX L – WEB RESOURCES

Resource	Link
ANSI International Committee for IT Standards	<a href="http://www.ncits.org">http://www.ncits.org</a>
Assistance to Firefighters Grants	<a href="http://firegrantsupport.com">http://firegrantsupport.com</a>
Catalog of Federal Domestic Assistance (CFDA)	<a href="http://12.46.245.173/cfda/cfda.html">http://12.46.245.173/cfda/cfda.html</a>
Citizen Corps Homepage	<a href="http://www.citizencorps.gov">http://www.citizencorps.gov</a>
Code of Federal Regulations	<a href="http://www.gpoaccess.gov/cfr/index.html">http://www.gpoaccess.gov/cfr/index.html</a>
Disability and Emergency Preparedness Resource Center	<a href="http://www.dhs.gov/disabilitypreparedness">www.dhs.gov/disabilitypreparedness</a>
Equipment Purchase Assistance Program	<a href="http://www.ojp.usdoj.gov/odp/docs/fs-padef.htm">http://www.ojp.usdoj.gov/odp/docs/fs-padef.htm</a>
Executive Order 12372	<a href="http://www.archives.gov/federal-register/codification/executive-order/12372.html">http://www.archives.gov/federal-register/codification/executive-order/12372.html</a>
HSEEP	<a href="http://hseep.dhs.gov">http://hseep.dhs.gov</a>
Federal Geographic Data Committee	<a href="http://www.fgdc.gov">http://www.fgdc.gov</a>
GAO Audits	<a href="http://www.gao.gov/govaud/ybk01.htm">http://www.gao.gov/govaud/ybk01.htm</a>
Goespatial One Stop Portal	<a href="http://www.GeoData.gov">http://www.GeoData.gov</a>
Grants Management System	<a href="https://grants.ojp.usdoj.gov">https://grants.ojp.usdoj.gov</a>
Lessons Learned Information System	<a href="https://www.LLIS.gov">https://www.LLIS.gov</a>
Limited English Proficiency	<a href="http://www.lep.gov">http://www.lep.gov</a>
MMRS Homepage	<a href="http://mmrs.fema.gov">http://mmrs.fema.gov</a>
Multi-State Information Sharing and Analysis Center	<a href="http://www.cscic.state.ny.us/msisac/index.html">http://www.cscic.state.ny.us/msisac/index.html</a>
National Information Exchange Model	<a href="http://www.niem.gov">http://www.niem.gov</a>
National Institute of Standards and Technology	<a href="http://www.nist.gov">http://www.nist.gov</a>
National Spatial Data Infrastructure	<a href="http://www.fgdc.gov/nsdi/nsdi.html">http://www.fgdc.gov/nsdi/nsdi.html</a>
National Strategy to Secure Cyberspace	<a href="http://www.whitehouse.gov/pcipb">http://www.whitehouse.gov/pcipb</a>
NIMS Information Center	<a href="http://www.fema.gov/nims">http://www.fema.gov/nims</a>
Office of Grants and Training Course Catalog	<a href="http://www.ojp.usdoj.gov/odp/training.htm">http://www.ojp.usdoj.gov/odp/training.htm</a>
Office of Grants and Training Secure Portal	<a href="https://odp.esportals.com">https://odp.esportals.com</a>
Office of Grants and Training SHSAS Resources	<a href="http://www.shsasresources.com">http://www.shsasresources.com</a>

Resource	Link
Office of Grants and Training Website	<a href="http://www.ojp.usdoj.gov/odp">http://www.ojp.usdoj.gov/odp</a>
OGO Financial Guide Ordering	<a href="http://puborder.ncjrs.org">http://puborder.ncjrs.org</a>
OJP Financial Guide	<a href="http://www.ojp.usdoj.gov/FinGuide">http://www.ojp.usdoj.gov/FinGuide</a>
OMB Circulars	<a href="http://www.whitehouse.gov/omb/circulars/index.html">http://www.whitehouse.gov/omb/circulars/index.html</a>
OMB e-gov initiatives	<a href="http://www.whitehouse.gov/omb/egov">www.whitehouse.gov/omb/egov</a>
Open Geospatial Consortium	<a href="http://www.opengeospatial.org">http://www.opengeospatial.org</a>
OSHA	<a href="http://www.osha.gov">http://www.osha.gov</a>
Pandemic Influenza Plan	<a href="http://www.hhs.gov/pandemicflu/plan">http://www.hhs.gov/pandemicflu/plan</a>
Ramona GIS Inventory	<a href="http://www.gisinventory.net">http://www.gisinventory.net</a>
Responder Knowledge Base	<a href="http://www.rkb.mipt.org">http://www.rkb.mipt.org</a>
SAFECOM	<a href="http://www.safecomprogram.gov/SAFECOM/grant/default.htm">http://www.safecomprogram.gov/SAFECOM/grant/default.htm</a>
Homeland Security Strategy Guidance	<a href="http://www.ojp.usdoj.gov/odp/assessments/definition.htm">http://www.ojp.usdoj.gov/odp/assessments/definition.htm</a>
Office of Grants and Training Technical Assistance	<a href="http://www.ojp.usdoj.gov/odp/ta.htm">http://www.ojp.usdoj.gov/odp/ta.htm</a>
The National Map	<a href="http://nationalmap.gov">http://nationalmap.gov</a>
First Responder Training Homepage	<a href="http://www.firstrespondertraining.gov">www.firstrespondertraining.gov</a>
U.S. Army Corps of Engineers CADD/GIS Technology Center Spatial Data Standards	<a href="http://tsc.wes.army.mil/products/TSSDS-TSFMS/tssds/html">http://tsc.wes.army.mil/products/TSSDS-TSFMS/tssds/html</a>
U.S. National Grid	<a href="http://www.fgdc.gov/standards/status/usng.html">http://www.fgdc.gov/standards/status/usng.html</a>
U.S. Computer Emergency Readiness Team	<a href="http://www.us-cert.gov">http://www.us-cert.gov</a>

**APPENDIX M:**

**ACRONYMS**

## APPENDIX M – ACRONYMS

### A

AAR	After Action Reports
ACH	Automated Clearing House
ADDIE	Analysis, Design, Development, Implementation, and Evaluation
AEL	Authorized Equipment List
AFG	Assistance to Firefighters Grant
ANSI	American National Standards Institute
APCO	Association of Public-Safety Communications Officials
ASAP	Automated Standard Application for Payments

### B

BSIR	Biannual Strategy Implementation Reports
BZPP	Buffer Zone Protection Plan

### C

CAP	Corrective Action Plan
CAPR	Categorical Assistance Progress Reports
CBP	Customs and Border Protection
CBRN	Chemical, Biological, Radiological and Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CCP	Citizen Corps Program
CCTV	Closed-Circuit Television
CDC	Centers for Disease Control and Prevention
CDP	Center for Domestic Preparedness
CEO	Chief Executive Officer
CERT	Community Emergency Response Teams
CFA	Capability Focus Area
CFR	Code of Federal Regulations
CFDA	Catalog of Federal Domestic Assistance
CI/KR	Critical Infrastructure/Key Resources
CIP	Critical Infrastructure Protection
CIRA	Catastrophic Incident Response Annex
CMIA	Cash Management Improvement Act
CME	Continuing Medical Education
CNE	Continuing Nursing Education
CO-OP	Cooperative Training Outreach Program
COTS	Commercial-off-the-Shelf
CSID	Centralized Scheduling and Information Desk

### D

D&B	Dun and Bradstreet
DHS	U.S. Department of Homeland Security

	DNDO	Domestic Nuclear Detection Office
	DOE	U.S. Department of Energy
	DOJ	U.S. Department of Justice
	DOS	U.S. Department of State
	DOT	U.S. Department of Transportation
	DPETAP	Domestic Preparedness Equipment Technical Assistance Program
	DUNS	Data Universal Numbering System
<b>E</b>		
	EA	Environmental Assessment
	EEG	Exercise Evaluation Guide
	EIS	Environmental Impact Statement
	ELO	Enabling Learning Objectives
	EMA	Emergency Management Agency
	EMAP	Emergency Management Accreditation Program
	EMI	Emergency Management Institute
	EMPG	Emergency Management Performance Grants
	EMS	Emergency Medical Services
	EMT	Emergency Medical Technician
	EOC	Emergency Operations Center
	EOP	Emergency Operations Plans
	EPA	U.S. Environmental Protection Agency
	EPW	Exercise Planning Workshop
<b>F</b>		
	FAR	Federal Acquisition Regulations
	FBI	Federal Bureau of Investigation
	FDA	Food and Drug Administration
	FE	Functional Exercise
	FEMA	Federal Emergency Management Agency
	FGDC	Federal Geographic Data Committee
	FICA	Federal Insurance Contributions Act
	FOIA	Freedom of Information Act
	FSE	Full-Scale Exercise
	FSR	Financial Status Report
	FTE	Full-Time Employees
<b>G</b>		
	G&T	Preparedness Directorate's Office of Grants and Training
	GAN	Grant Adjustment Notice
	GAO	Government Accountability Office
	GEA	Geospatial Enterprise Architecture
	GIS	Geographic Information System
	GISWG	Global Infrastructure and Standards Working Group

GJXDM Global Justice XML Data Model  
 GML Geography Markup Language  
 GMS Grants Management System  
 GOTS Government-off-the-Shelf  
 GPS Global Positioning Systems

**H**

HAZMAT Hazardous Materials  
 HDER Homeland Defense Equipment Reuse  
 HHS U.S. Department of Health and Human Services  
 HRSA Health Resources and Services Administration  
 HSC Homeland Security Council  
 HSEEP Homeland Security Exercise and Evaluation Program  
 HSGP Homeland Security Grant Program  
 HSIN Homeland Security Information Network  
 HSOC Homeland Security Operations Center  
 HSPD Homeland Security Presidential Directive  
 HSPTAP Homeland Security Preparedness Technical Assistance Program  
 HSVAC Homeland Security Virtual Assistance Center

**I**

IAB InterAgency Board  
 IAFIS Integrated Automated Fingerprint Identification System  
 IAIP Information Analysis and Infrastructure Protection Directorate  
 IBSGP Intercity Bus Security Grant Program  
 ICS Incident Command System  
 ICTAP Interoperable Communication Technical Assistance Program  
 IED Improvised Explosive Device  
 IEEE Institute of Electrical and Electronics Engineers, Inc.  
 INCITS International Committee for Information Technology Standards  
 IP Improvement Plan  
 IPRSGP Intercity Passenger Rail Security Grant Program  
 ISAC Information Sharing and Analysis Center  
 ISIP Initial Strategy Implementation Plan  
 ISO International Standards Organization  
 IWN Integrated Wireless Network

**J**

JRIES Joint Regional Information Exchange System  
 JTTF Joint Terrorism Task Force

**L**

LAP Lesson Administration Page  
 LEP Limited English Proficient  
 LETPP Law Enforcement Terrorism Prevention Program

LLEA	Lead Law Enforcement Agency
LLIS	Lessons Learned Information Sharing
LMR	Land Mobile Radio
LNG	Liquid Natural Gas
LOCES	Letter of Credit Electronic Certification System

## M

M&A	Management and Administrative
MEDS	Minimum Essential Data Sheets
MIPT	National Memorial Institute for the Prevention of Terrorism
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MMRS	Metropolitan Medical Response System
MRC	Medical Reserve Corps
MS&G	Models, Simulations, and Games

## N

NCIC	National Crime Information Center
NCJA	National Criminal Justice Association
NCR	National Capital Region
NDPC	National Domestic Preparedness Consortium
NEPA	National Environmental Policy Act
NFA	National Fire Academy
NFPA	National Fire Protection Association
NGA	Notice of Grant Award
NGO	Non-Governmental Organization
NIC	NIMS Integration Center
NIEM	National Information Exchange Model
NIMCAST	NIMS Capability Assessment Support Tool
NIMS	National Incident Management System
NIOSH	National Institute for Occupational Safety and Health
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NRP	National Response Plan
NSDI	National Spatial Data Infrastructure
NSGIC	National States' Geographic Information Council
NSSE	National Special Security Event

## O

OC	Office of the Comptroller
ODP	Office for Domestic Preparedness
OIC	Office for Interoperability and Compatibility
OJP	Office of Justice Programs
OGC	Office of General Counsel

	OGC™	Open Geospatial Consortium
	OGO	Office of Grant Operations
	OMB	Office of Management and Budget
	OSHA	Occupational Safety and Health Administration
<b>P</b>		
	PAPRS	Phone Activated Paperless Request System
	PHS	Public Health Service
	POC	Point of Contact
	POETE	Plan, Organize, Equip, Train, Exercise
	POI	Point of Interest
	PPE	Personal Protective Equipment
	PSGP	Port Security Grant Program
	PSTN	Public Switched Telephone Network
<b>R</b>		
	RAD/NUC	Radiological and Nuclear
	RAT	Rapid Assistance Team
	RDT&E	Research, Development, Testing and Evaluation
	RKB	Responder Knowledge Base
	RTSWG	Region Transit Security Working Group
<b>S</b>		
	S&T	Science and Technology
	SAA	State Administrative Agency
	SAAT	Standardized Awareness Authorized Trainer
	SDSFIE	Spatial Data Standard for Facilities, Infrastructure, and Environment
	SEL	Standardized Equipment List
	SHSAS	State Homeland Security Assessments and Strategies
	SHSEEP	State Homeland Security Exercise and Evaluation Program
	SHSP	State Homeland Security Program
	SLGCP	Office of State and Local Government Coordination and Preparedness
	SME	Subject Matter Expert
	SOP	Standard Operating Procedure
	SoR	Statement of Requirements
	SPOC	Single Point of Contact
	SRM	Service Reference Model
	SWAT	Special Weapons and Tactics
<b>T</b>		
	TA	Technical Assistance
	TCL	Target Capabilities List
	TEW	Terrorism Early Warning
	TLO	Terminal Learning Objectives
	TOPOFF	Top Officials Exercise



	TPOC	Training Point of Contact
	TRM	Technical Reference Model
	TSGP	Transit Security Grant Program
	TSP	Training Support Package
	TTX	Tabletop Exercise
<b>U</b>		
	UASI	Urban Areas Security Initiative
	UAWG	Urban Area Working Group
	UHF	Ultra High Frequency
	USAR	Urban Search and Rescue
	USDA	U.S. Department of Agriculture
	USGS	U.S. Geological Survey
	UTL	Universal Task List
<b>V</b>		
	VHF	Very High Frequency
	VIPS	Volunteers in Police Service
<b>W</b>		
	WFS	Web Feature Service
	WMD	Weapons of Mass Destruction
	WMS	Web Map Service
<b>X</b>		
	XML	Extensible Markup Language
	XSTF	XML Structure Task Force

**APPENDIX N:**

**INDEX**

## APPENDIX N – INDEX

- Allowable Costs, 31
- Authorized Equipment List (AEL), 25, 34, 72, 84, 90, 102, 110
- Authorized Program Expenditures, v, 70, 80, 87, 101, 107
- Award Date, 63, 79, 94
- Biannual Strategy Implementation Reports (BSIR), 65, 67, 70, 101, 107
- Capability Focus Area (CFA), 94, 96, 97, 98, 99, 103
- Catastrophic, 11, 13, 20, 22, 35, 36, 37, 42, 69, 70, 71, 72, 73, 76, 77, 80, 81, 84, 94, 103
- Catastrophic Planning, 11
- CBRNE, 9, 17, 35, 42, 49, 69, 73, 76, 84, 87, 90, 95, 96, 97, 98, 102, 110
- Centers for Disease Control and Prevention (CDC), 19, 20, 21, 97, 103, 104
- Centralized Scheduling and Information Desk (CSID), 48, 49
- Citizen Corps Councils, 22, 23, 27, 35, 71, 80, 91, 103, 106, 107, 108, 109
- Citizen Corps Program (CCP), iii, iv, 1, 17, 22, 27, 32, 35, 47, 52, 53, 54, 55, 60, 106, 107, 110, 112
- Citizen Participation, 23, 44, 71, 80, 88, 103, 106, 107, 108
- Code Orange, 32, 33, 82, 88
- Code Yellow, 32, 82, 88
- Construction and Renovation, 47, 48, 104, 112
- Critical Infrastructure Protection, 71, 81, 87, 88, 91
- Cyber Security, 90
- Domestic Nuclear Detection Office (DNDO), iii, 10
- DUNS number, 58
- Enhancement Plan, 53, 59, 60, 78
- Equipment, iv, 8, 19, 31, 34, 45, 50, 72, 73, 84, 90, 102, 107, 110
- Exercises, v, 8, 31, 35, 41, 42, 43, 44, 65, 73, 84, 91, 102, 107, 111
- Extensible Markup Language, 24
- Financial Status Report (FSR), 64, 67
- Freedom of Information Act (FOIA), 29
- Health Resources and Services Administration (HRSA), 19, 20, 21, 97
- Homeland Security Exercise and Evaluation Program (HSEEP), 41, 42, 43, 44, 45, 50, 63, 65, 66, 85, 95, 102, 103, 104, 111
- Homeland Security Presidential Directive, 3, 5
- Homeland Security Strategy, 16, 37, 43, 60, 70, 77, 78, 79, 85, 91, 101
- HSPD-8, 96
- Interoperable Communications, iv, 8, 9, 50, 73, 84, 90, 97, 98, 102
- Investment Justification, iii, 14, 32, 35, 53, 59, 60, 61, 78, 82, 88
- Katrina, 4, 5, 11, 69, 76, 97
- Law Enforcement Terrorism Prevention Program (LETPP), iii, iv, v, 1, 17, 20, 22, 27, 32, 33, 35, 42, 47, 52, 53, 54, 57, 60, 83, 87, 88, 89, 90, 91, 92
- Lessons Learned Information Sharing (LLIS), 49
- Limited English Proficient (LEP), 30
- Management and Administrative (M&A), v, 31, 45, 46, 47, 74, 85, 92, 104, 107, 112
- Memorandum of Understanding, iii, 28
- Metropolitan Medical Response System (MMRS), iii, iv, 1, 17, 22, 27, 32, 35, 46, 47, 52, 53, 54, 55, 59, 60, 77, 78, 94, 95, 96, 97, 98, 100, 101, 102, 103, 104
- Monitoring, 63, 66
- National Environmental Policy Act (NEPA), 47, 48
- National Incident Management System (NIMS), iii, iv, 2, 3, 5, 6, 9, 16, 19, 31, 40, 41, 70, 71, 73, 80, 88, 90, 91, 97, 98, 110

National Infrastructure Protection Plan (NIPP), 2, 3, 4, 5, 6, 7

National Preparedness Goal, ii, 1, 3, 4, 5, 11, 12, 13, 14, 16, 21, 22, 31, 41, 49, 52, 53, 60, 70, 73, 78, 80, 84, 87, 94, 95, 96, 101, 102, 106

National Response Plan (NRP), 2, 3, 4, 5, 11, 13, 16, 19, 42, 69, 70, 72, 73, 76, 77, 80, 81, 102

OJP Financial Guide, 49, 65

Pandemic Influenza, 4, 99, 100

Period of performance, 27, 33, 83, 89, 94

Planning, iv, 4, 10, 12, 13, 20, 24, 30, 31, 32, 38, 43, 69, 70, 71, 76, 80, 87, 88, 101, 107, 108

Private Sector, 5, 7, 14, 17, 19, 23, 26, 35, 70, 71, 76, 81, 87, 107, 110

Program and Capability Review, 53, 59, 78

Program Requirements, v, 70, 77, 95, 107

Public Awareness, 109

Reporting Requirements, iii, 63, 64, 107

Responder Knowledge Base (RKB), 34, 72, 84, 90, 102, 110

SAFECOM, 9

Senior Advisory Committee (SAC), 21

SF-424, 57

State Homeland Security Program (SHSP), iii, iv, v, 1, 16, 20, 22, 27, 32, 35, 42, 43, 46, 47, 52, 53, 54, 57, 59, 60, 69, 70, 72, 73, 74, 80, 107

Target Capabilities, iii, iv, 1, 12, 21, 37, 41, 44, 60, 69, 73, 84, 87, 94, 95, 96, 98, 101, 104

Target Capabilities List (TCL), 1, 2, 3, 12, 13, 14, 16, 20, 21, 34, 37, 38, 42, 44, 69, 76, 91, 96, 103, 106

Technical Assistance, 49, 98

Training, ii, iv, 6, 8, 17, 19, 20, 21, 31, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 48, 50, 73, 79, 83, 84, 85, 89, 90, 91, 101, 102, 103, 107, 110

Training and Exercise Plan, 40, 41, 42, 43, 44, 85, 102, 103

Transit Security Grant Program (TSGP), 5, 18, 22, 23

Unallowable Costs Guidance, 48

Universal Task List, 37, 44

Urban Area Security Initiative (UASI), iv, v, 1, 5, 9, 16, 22, 27, 32, 33, 35, 42, 43, 47, 50, 52, 53, 54, 57, 58, 59, 60, 76, 77, 78, 79, 80, 82, 83, 84, 85, 89