



**Colorado Department of Local Affairs  
Division of Emergency Management**

**2006**

**Notice of Available Homeland Security Funds**

**Fiscal Year (FY) 2006 State Homeland Security Program (SHSP)  
Law Enforcement Terrorism Prevention Program (LETPP)  
Urban Area Security Initiative (UASI)  
Citizen Corp Program (CCP)  
Metropolitan Medical Resource System (MMRS)**

<b>Contents</b>	<b>Page</b>
I. Introduction and Background	3
II. Program Guidance	5
III. Applications	6
IV. Management and Administration	7
V. Equipment Costs Guidance	7
VI. Training Costs Guidance	8
VII. Exercise Costs Guidance	12
VIII. Personnel: Hiring, Overtime and Backfill Guidance	16
IX. Unallowable Costs	17
X. Information and Technology Guidance	17
XI. Additional State Requirements and Guidance	19
XII. Coordination Requirements	20
XIII. Minimum FY06 NIMS Compliance	21
XIV. State Homeland Security Program	22
XV. Law Enforcement Terrorism Prevention Program (LETPP)	26
XVI. Urban Area Security Initiative (UASI)	30
XVII. Citizen Corps Program (CCP)	37
XVIII. Metropolitan Medical Response System	42
XIX. References	43
Time Table	44
Contacts	44

# I. Introduction and Background

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]), Colorado will receive grant funding based on risk and need to build capabilities and enhance homeland security.

The 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 the Nation's priorities and focus expenditures. This common planning framework and the supporting tools help us to better understand how prepared we are, how prepared we need to be, and how to prioritize efforts to close the gap.

The Colorado Department of Local Affairs (DOLA) announces the availability of funding for the 2006 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).

As in previous fiscal years, the FY06 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 Colorado.

The FY06 HSGP highlights the Interim National Preparedness Goal. The Goal presents a collective vision for national preparedness and establishes national priorities to guide the realization of that vision to meet the most urgent needs. Tools supporting the Goal include:

- National Planning Scenarios
- Universal Task List
- Target Capabilities
- National Response Plan (NRP)
- National Incident Management System (NIMS)
- Interim National Infrastructure Protection Plan (NIPP)
- Colorado State and UASI Homeland Security Strategies

These documents should guide FY06 HSGP applications to more effectively address the gaps between needs, risks and existing capabilities. Funds made available through the FY06 HSGP will focus on seven priorities. The first three overarching priorities contribute to the development of multiple capabilities:

### ***Three Overarching Priorities***

1. Expanded Regional Collaboration
2. Implement NIMS and NRP
3. Implement NIPP

The last four priorities build on selected capabilities for which the Nation has the greatest need and for which eight priority capabilities have been identified:

Four National Priorities	Eight Priority Capabilities
4. Strengthening Information Sharing and Collaboration Capabilities	<ul style="list-style-type: none"> <li>• Information Sharing and Dissemination Law</li> <li>• Enforcement Investigation and Operations</li> </ul>
5. Strengthening Interoperable Communications Capabilities	<ul style="list-style-type: none"> <li>• Interoperable Communications</li> </ul>
6. Strengthening CBRNE Detection Response and Decontamination Capabilities	<ul style="list-style-type: none"> <li>• CBRNE Detection</li> <li>• Explosive Device Response Operations</li> <li>• MD/Hazardous Materials Response and Decontamination</li> </ul>
7. Strengthening Medical Surge and Mass Prophylaxis Capabilities	<ul style="list-style-type: none"> <li>• Mass Prophylaxis</li> <li>• Medical Surge</li> </ul>

The state will determine its strengths and weaknesses through prioritization of up to fifteen capabilities identified at the Program Review on January 10-11, 2006. The thirteen capabilities will consist of the eight National Priority Capabilities listed above, as well as additional capabilities identified by the state through a regional and state capability assessment and discussion at the Program Review.

The U.S. Department of Homeland Security, Office for Domestic Preparedness FY06 grant funding was structured to include several programs for funding. In the Program Guidance, the following five programs are available for application: SHSP, LETPP, UASI, MMRS, and CCP. One grant application will be accepted for each program area, however; only the Denver Urban Area is eligible for the UASI funding. Funding for MMRS will receive a baseline allocation while the other four programs will be awarded funding based on risk and need. Funds will be distributed with 20% for state initiatives and 80% for local initiatives.

Colorado Division of Emergency Management (DEM) is requiring interested applicants for the 2006 SHSP, LETPP, MMRS, and CCP to submit one regional application through the nine (9) Colorado All-Hazards Emergency Management Regions (AHEMR), established pursuant to **Executive Order D 013 03** issued by Colorado Governor Bill Owens (Exhibit A). A state map is attached that outlines each county and Tribal Nation (where applicable) within each region. One application will be accepted for UASI, and one application will be accepted from each participating state department.

In December 2005, ODP released guidance on conducting a program and capability review, a key building block in the process states will use to develop their Investment Justification for FY 2006 funds. As part of the State application process, States are required to submit summary results of their Program and Capability Review based on regional and state input received January 10-11, 2006, as well as Investment Justification narrative.

The process for the AHEMR and state agencies will be as follows:

01-05-2006	Program Capability Review of the 36 capabilities, AHEMR and the State must submit the completed reviews to CU
01-11-2006	Program Capability Review (10 <sup>th</sup> and 11 <sup>th</sup> )
02-06-2006	State, UASI, and Regional draft applications due (UASI must submit an investment justification and narrative for each initiative for 2006 funding)
03-02-2006	Colorado submits application to ODP for 2006 Homeland Security Funding
03-06-2006	Technical Assistance for state and regional applications
04-03-2006	Regional and State Departments FINAL applications due
05-08-2006	Regional Presentation of 2006 applications (8 <sup>th</sup> 9 <sup>th</sup> 10 <sup>th</sup> )
06-15-2006	Grants awarded
07-01-2006	Grant Award Start Date

DEM staff will review “Draft Applications” for technical and project eligibility. DEM staff will provide technical assistance, including clarification and recommendations for each application. The “Draft Application” will be returned on or before March 6<sup>th</sup>, 2006. The “Final Application” is due from each Region/State Agency on April 3, 2006.

In May AHEMR will present their applications to the Homeland Security Advisory Committee. The Committee will review all the applications and will provide funding recommendations to the Executive Director of DOLA.

## II. Program Guidance

Colorado will employ a regional approach to meet the needs identified through the assessments and in the Colorado State Homeland Security Strategy.

In contrast to other years, this year marks a significant change in the way in which Homeland Security Grant Program funds are allocated. The State and Homeland Security Program (SHSP), the Urban Area Security Initiative (UASI), the Law Enforcement Terrorism Prevention Program (LETPP), and the Citizen Corps Program (CCP) will receive funding competitively based on risk and need. The Metropolitan Medical Response System (MMRS) program will receive baseline allocation funding.

Furthermore, the state intends to guide state, regional, and local security and preparedness efforts toward a project-oriented process. 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.

To assist AHEMR and state agencies in addressing the gaps between needs, risks and existing capabilities, the following documents should be utilized:

- The Interim National Preparedness Goal
- National Planning Scenarios
- Universal Task List
- Target Capabilities
- National Response Plan (NRP)
- National Incident Management System (NIMS)
- Interim National Infrastructure Protection Plan (NIPP)

In addition to the documents listed above, funding requests must be aligned with the Colorado State Homeland Security Strategy Goals:

### **GOAL 1: Planning**

Enhance the planning process for the state strategy to ensure it mirrors the National Response Plan (NRP) and incorporated the National Preparedness Goal and Guidance.

### **GOAL 2: Training and Exercises**

Through training and exercises, improve Colorado’s ability to deal with terrorist-related incidents.

### **GOAL 3: Information Sharing**

Facilitate the prevention of terrorism by enhancing the abilities of state and local agencies to gather, analyze, and share information.

### **GOAL 4: Communications Interoperability**

Develop a statewide standards based comprehensive interoperable communication system that provides instant and disruption-resistant communications capabilities for all public safety and first responder agencies.

### **GOAL 5: Critical Infrastructure Protection**

Identify and prioritize critical infrastructure, key assets, and high-population density venues pursuant to the principles of the National Strategy for Homeland Security (NSHS) and the National Infrastructure Protection Plan (NIPP).

**GOAL 6: Cyber Security**

Prevent and deter widespread disruption and damage caused by cyber attacks on Colorado's critical infrastructure.

**GOAL 7: Food and Agriculture Protection**

Provide the Colorado food and agriculture sectors with the guidance to prepare, prevent, respond, and recover from agro-terrorist attacks.

**GOAL 8: Public Health Protection**

Provide an effective response and coordinated patient care that protects the health of Colorado citizens in the event of a terrorist attack.

**GOAL 9: Citizen Participation**

Strive to include Colorado citizens in homeland security activities through public education and outreach, training, and volunteer service opportunities.

**GOAL 10: Continuity of Government**

Develop a continuity of government focusing on constitutional governance, ensuring command and control of response and recovery operations, and facilitating the restoration of critical and essential services expected by Colorado citizens.

**GOAL 11: Emergency Responder Capabilities**

Colorado will build capacity to equip, train, and effectively manage first responder resources for terrorism events.

**Any references made to "Appendices A-N" in this document, indicate attachments to the "FY2006 Homeland Security Grant Program: Program Guidance and Application Kit" located at: <http://www.ojp.usdoj.gov/odp/docs/fy2006hsgp.pdf>.**

### III. Applications

AHEMR must submit one application for each funding area (SHSG, LETPP, and CCP). Jurisdictions in the Counties of Denver, Adams, Arapahoe, and Jefferson are eligible for UASI funds and will submit one application for UASI funds; all other applications must be submitted by AHEMR. State Departments may submit one application for the Department coordinated through the Executive Director's Office. Applications are available on the DEM web site <http://www.dola.state.co.us/oem/oemindex.htm>. The ISIP template will be required from each AHEMR, UASI, and State Department.

**Step one:**

Questions on applications, equipment, training, exercise, planning, and or processes should be submitted via email to Carmen Velasquez at [Carmen.Velasquez@state.co.us](mailto:Carmen.Velasquez@state.co.us) by **February 6, 2006**. Answers to all questions will be posted on <http://www.dola.state.co.us/oem/oemindex.htm> DEM website.

**Step two:**

Each Region is required to submit a **DRAFT APPLICATION** by **5:00 pm, February 6, 2006** to DEM, 9195 East Mineral Ave. Centennial, CO 80112. The **DRAFT APPLICATION** will enable DEM staff to review eligibility of each project and offer technical assistance (TA) to each region in order to optimize the regional application and ensure appropriate projects are included in each application.

**Step three:**

Applications will be returned to each AHEMR and UASI with recommendations by **March 6, 2006**.

**Step four:**

AHEMR, UASI and State Departments will submit a detailed **Final Application** by **5:00pm** April 3, 2006 to DEM, Attention: Carmen Velasquez, 9195 East Mineral Ave. Centennial, CO 80112. Each AHEMR and UASI will present applications to the Homeland Security Grant Advisory

Committee on **May 8, 9 and 10, 2006**. Additional information will be sent to each Region and UASI on presentation schedules. **(Note: Four original applications must be submitted with original signatures)**

**Step five:**

AHEMR will receive award letters from DOLA based on the available Homeland Security Funds.

## **IV. Management and Administrative (M&A)**

All programs within FY 2006 HSGP have allowable M&A costs for both the State as well as local units of government. No more than 5% of the total State program amount allocated within FY 2006 HSGP may be retained at the State level and used for M&A purposes. In addition, subgrantees may retain and use up to 3% of their subaward from the State for local M&A purpose.

AHEMR must include a detailed budget for the Homeland Security Regional Coordinator, operating expenses, and any other administrative expenses. This is a multi-disciplinary/multi-jurisdictional approach and must engage participation from all disciplines: law enforcement, public health, health care, emergency management, government administration, public works, fire service, emergency medical services, hazardous materials, and public safety communications.

## **V. Equipment Costs Guidance**

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 website along with separate listings for the FY 2005 AEL and the Fall 2005 Standardized Equipment List (SEL). In some cases, items that were eligible under the FY 2005 grant guidelines that were listed on the SEL are not allowable under FY 2006 HSGP or will not be eligible for purchase unless specific conditions are met. Examine the list carefully as some new items are eligible under FY 2006 HSGP that were 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.

The twenty-one (21) allowable categories of equipment under FY 2006 HSGP are listed in Appendix D. 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 the "Other Authorized Equipment" section for specific guidance. Maintenance costs/contracts for authorized equipment purchased using FY 2006 HSGP funding or acquired through Homeland Defense Equipment Reuse (HDER) Program are allowable, unless otherwise specified.

In order to qualify for radio communications equipment, a region must have identified a planning process and documented a regional communications plan. The communications plan must achieve interoperable communications across jurisdictions including regional and state. The plan must also include a training

and exercise component. Funded items must show a significant improvement in interoperable communication.

*Note: In an effort to improve emergency preparedness and response interoperability, all new or upgraded radio systems and new radio equipment **must** be compatible with a suite of standards called ANSI/TIA/EIAA-102 Phase I (Project 25). These standards have been developed to allow for backward compatibility with existing digital and analog systems and provide for interoperability in future systems. The FCC has chosen the Project 25 suite of standards for voice and low-moderate speed data interoperability in the new nationwide 700 MHz frequency band. The Integrated Wireless Network (IWN) of the U.S. Justice and Treasury Departments has also chosen the Project 25 suite of standards for their new radio equipment. In an effort to realize improved interoperability, all radios purchased under this grant **must** be APCO 25 compliant.*

Any questions concerning the eligibility of equipment not addressed in the AEL should be directed to the appropriate DOLA/DEM Program Manager. All expenditures and items in the application must be allowable according to <http://www.ojp.usdoj.gov/odp/docs/fy2006hsgp.pdf>.

## **VI. Training Costs Guidance**

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 include the establishment, support, conduct, and attendance for training programs specifically identified under the SHSP, UASI, LETPP, MMRS, and CCP grant programs.

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 from 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 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 become self-sustaining.

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.

A Regional Training plan and budget are required for 2006 funding. Activities must address shortfalls and gaps identified within each region. The plan should align with the Homeland Security Strategy.

### **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 and have the approval of DOLA/DEM.
  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 DOLA/DEM. Such costs must be included within the funding allowed for program management personnel expenses, which must not exceed 15% of the total allocation.

### ***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. Please note Web-Forms moved 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 this year. 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 should 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 using the list of disciplines: 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 should include all of the materials associated with the delivery of the training course. Items that should consist of:
  - a. **Instructor Guide/Instructor Outline/Instructor Lesson Plans.** The published instructor materials that contain course texts and special instructor notes that provide the necessary information to deliver the material.
  - b. **Participant Manual/Guide/Workbook.** The published student materials that contain 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.** Descriptions of practical exercises, tabletop exercises, hands-on exercises or other material that support 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 use 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 and 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. DOLA/DEM will conduct periodic reviews of all State, Region, and Urban Area funded training. These reviews may include requests for all course materials (POI/TSP), 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 must demonstrate linkage to a Target Capability and be applicable to the State, Region, 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 in the exercises discussion in the 2006 ODP announcement section D.5.

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

This year's HSGP includes the G&T Cooperative Training Outreach Program (CO-OP), 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.

Any questions concerning the eligibility of training not addressed here should be directed to the appropriate DOLA/DEM Program Manager. All expenditures and items listed in the application must be allowable according to <http://www.ojp.usdoj.gov/odp/docs/fy2006hsgp.pdf>.

## **VII. 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). 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>.

A Regional Exercise plan and budget are required for 2006 funding. Activities must address shortfalls and gaps identified within each region. The plan should align with the Homeland Security Strategy.

### ***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 during which they should 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, AHEMR should identify training and exercise priorities that align with the Homeland Security Strategies and map the 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, and end 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.

AHEMR are also encouraged to develop a schedule within the Training and Exercise Plan that takes into consideration anticipated training needs of the Region 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 Region, and to ensure the scheduling of both training and exercises are based on national and State priorities. 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). The AAR/IP ensures 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 has been broadened to include natural and technological disasters in addition to terrorism (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, resulting 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 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 tailor the scenario 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.

### **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, educational opportunities identified 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 and these revisions should be finalized by the 1st quarter 2006. In the interim the current HSEEP EEGs and AAR/IP template should be utilized.

AAR/IPs must be provided to DEM within 30 days following the completion of each exercise (see HSEEP Volume IV for sample AAR/IP template).

In order to leverage assessments to ensure the gathering of objective exercise-based data, AHEMR 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***

AHEMR are expected to develop a self-sustaining State Homeland Security Exercise and Evaluation Program. This may include: 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.

Training on the use and implementation of HSEEP is being offered to States and Territories. It includes independent study and mobile course curriculum on the creation 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** –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 DOLA/DEM. Such costs must be included within the funding allowed for program management personnel expenses and must not exceed 15% of the total allocation. The services of contractors/consultants may also be procured to support the design, development, conduct and evaluation of exercises, but these contracts **must** be pre-approved by DOLA/DEM.
- **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 planning and conducting 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 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.***
- Equipment that is purchased for permanent installation and/or use, beyond the scope of exercise (e.g., electronic messaging signs).

Any questions concerning the eligibility of exercises not addressed here should be directed to the appropriate DOLA/DEM Program Manager. All expenditures and items listed in the application must be allowable according to <http://www.ojp.usdoj.gov/odp/docs/fy2006hsgp.pdf>.

## **VIII. Personnel: Hiring, Overtime, and Backfill Guidance**

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 only hire staff for program management functions not operational duties.

The hiring of planners, training program coordinators, exercise managers, and grant administrators falls 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. Furthermore, 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.

## IX. Unallowable Costs Guidance

Several costs are strictly prohibited under FY 2006 HSGP. Grantees should contact DOLA/DEM for guidance and clarification.

### 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.

## X. Information Technology Guidance

### *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 all schemas (extensions, constraint, proxy) generated as a result of this grant available without restriction, 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. AHEMR and State Departments will work together in developing the protocols, procedures, and agreements necessary for exchanging critical homeland security data with the state in the event of an incident, training or exercise. AHEMR and State Departments will share GIS information as a requirement to prevent, protect against, respond to, and recover from terrorist activity, major disasters, and other emergencies in Colorado, and or incidents of national significance.

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, with 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 of 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.

## **XI. Additional State Requirements and Guidance**

1. Successful applicants must participate in the Colorado Statewide Emergency Resources Ordering Status System (ROSS) and submit resource information for inclusion in the ROSS database.
2. Fire Departments or entities providing fire protection that receive funding under the Homeland Security Grant Program must provide incident information to the National Fire Incident Reporting System (NFIRS), administered by the Colorado Division of Fire Safety.
3. AHEMR and State Departments will work together in developing the protocols, procedures, and agreements necessary for exchanging critical homeland security data with the state in the event of an incident, training or exercise. AHEMR and State Departments will share GIS information as a requirement to prevent, protect against, respond to, and recover from terrorist activity, major disasters, and other emergencies in Colorado, and or incidents of national significance.
4. Purchases made with Homeland Security funds must follow local procurement procedures, or procurement procedures as required by statute, ordinance, and or executive orders.
6. In order to qualify for radio communications equipment, a region must have an identified planning process and a documented regional communications plan. The communications plan must

achieve interoperable communications across jurisdictions including regional and state. The plan must also include a training and exercise component. Funded items must show a significant improvement in interoperable communication.

## XII. Coordination Requirements

### ***Citizen Coordination***

AHEMR must coordinate with UASI and the State for citizen participation in preparedness and educational programs (i.e. Ready Colorado). Citizens are a critical component in securing the homeland. In order to have a prepared and protected community and Nation, citizens should 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 Colorado* Campaign, DOLA 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 prepared America.

In support of this mission, all SHSP, UASI, LETPP, CCP, and MMRS award recipients should 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, to integrate citizen/volunteer resources and participation, and to 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, AHEMR must include an integrated approach to engaging citizens in preparedness, training, exercises, and volunteer support for emergency responders through Citizen Corps Councils. AHEMR are encouraged to fully leverage HSGP resources to accomplish this integration.

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

AHEMR and the Urban Area 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.

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

Grantees should work closely to engage the EMS community in preparedness efforts. 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. AHEMR and UASI **not providing at least ten percent of its grant funding to EMS providers** should be prepared to provide an explanation supporting EMS funding decisions to DOLA.

## **XIII. Minimum FY06 NIMS Compliance Requirements**

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 between 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.

## **XIV. 2005 State Homeland Security Program**

SHSP is a core homeland security assistance program providing 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 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 Target Capability List (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 bio-terrorism preparedness effort offers another example. Grantees must demonstrate the dual-use nature of any activities implemented under this program not explicitly focused on terrorism preparedness.

### ***Program Requirements***

Use of SHSP funds must be consistent with and supportive of implementation of the State Homeland Security Strategy.

Any questions concerning the eligibility of SHSP not addressed should be directed to the appropriate DOLA/DEM Program Manager. All expenditures and items listed in the application must be allowable according to <http://www.ojp.usdoj.gov/odp/docs/fy2006hsgp.pdf>.

### ***Authorized Program Expenditures***

This section provides guidance on the types of expenditures that are allowable under the SHSP.

### **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:
  - Implementing the National Preparedness Goal and Guidance.
  - Implementing and adopting NIMS.
  - Modifying existing incident management and emergency operating procedures to ensure proper alignment with the NRP coordinating structures, processes, and protocols.
  - Establishing or enhancing mutual aid agreements.
  - Developing communications and interoperability protocols and solutions.
  - Conducting local, regional, and Tribal program implementation meetings.
  - Developing or updating resource inventory assets in accordance to typed resource definitions issued by the NIMS Integration Center (NIC).
  - Designing State and local geospatial data systems.
  - 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:
  - Planning to enhance security during heightened alerts, during terrorist incidents, and/or during mitigation and recovery.
  - Multi-discipline preparation across first responder community, including EMS for response to catastrophic events and acts of terrorism.
  - Public information/education: printed and electronic materials, public service announcements, seminars/town hall meetings, web postings coordinated through local Citizen Corps Councils.
  - Citizen Corps volunteers programs and other activities to strengthen citizen participation.
  - 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.
  - Evaluating CIP security equipment and/or personnel requirements to protect and secure sites.
  - 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:
  - Developing or enhancing emergency operating procedures and operating procedures.
  - Developing terrorism prevention/deterrence plans.
  - 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.
  - Developing or enhancing border security plans.
  - Developing or enhancing cyber security plans.
  - Developing or enhancing cyber risk mitigation plans.
  - Developing or enhancing agriculture/food security risk mitigation, response, and recovery plans.
  - Developing public/private sector partnership emergency response, assessment, and resource sharing plans.
  - Developing or updating local or regional communications plans.
  - Developing plans to support and assist special needs jurisdictions, such as port authorities and rail and mass transit agencies.

- Developing or enhancing continuity of operations and continuity of government plans.
- Developing or enhancing existing catastrophic incident response and recovery plans to include and integrate Federal assets provided under the NRP.
- Developing or enhancing evacuation plans.
- Developing or enhancing citizen surge capacity.
- Developing or conducting assessments, including but not limited to:
  - Conducting point vulnerability assessments at critical infrastructure sites/key assets and develop remediation/security plans.
  - Conducting cyber risk and vulnerability assessments.
  - 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.
  - 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).
  - Activities that directly support the identification of pre-designated temporary housing sites.

**Equipment**

FY 2006 SHSP funds may be used for equipment acquisition from the twenty-one (21) equipment categories listed in the FY 2006 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.

**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		

**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. 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

### **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.

### **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 10% 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). 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.

### **Management and Administration**

Local jurisdiction subgrantees may retain and use up to 3 percent of their subaward from the State for local M&A purposes.

### ***SHSP Target Capabilities***

- Planning
- Community Preparedness and Participation
- Communications
- Risk Management
- Information 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 & Agriculture 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 Information & 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 & Decontamination
- Structural Damage Assessment & Mitigation
- Economic & Community Recovery
- Restoration of Lifelines

## **XV. 2006 Law Enforcement Terrorism Prevention Program**

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.

The AHEMR 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.

### ***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.

Any questions concerning the eligibility of LETPP not addressed should be directed to the appropriate DOLA/DEM Program Manager. All expenditures and items listed in the application must be allowable according to <http://www.ojp.usdoj.gov/odp/docs/fy2006hsgp.pdf>.

### ***Authorized Program Expenditures***

FY 2006 LETPP funding is expended based on the State Homeland Security Strategies.

### **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:
  - o Planning for enhancing security during heightened alerts, terrorist incidents, and/or mitigation and recovery.
  - o Public information/education: printed and electronic materials, public service announcements, seminars/town hall meetings, web postings.
  - o Citizen Corps volunteer programs and other activities to strengthen citizen participation.
  - o Evaluating CIP security equipment and/or personnel requirements to protect and secure sites.

### **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.

**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 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.

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 closeout 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.***

### **Equipment**

LETPP funds may be used for equipment acquisition from the LETPP 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 – LETPP Allowable Equipment Categories**

<b>Cat. #</b>	<b>Category Title</b>	<b>Cat. #</b>	<b>Category Title</b>
[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

### **Training**

LETPP 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.

### **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.

### **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 10% 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). 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.

### **Management and Administration**

Local jurisdiction subgrantees may retain and use up to 3 percent of their subaward from the State for local M&A purposes.

### ***LETPP 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

## **XVI. 2006 Urban Areas Security Initiative (UASI)**

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 bio-terrorism 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, resulting 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 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 the 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 identify Urban Area authorities through the SAAs. 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.

### ***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.

Any questions concerning the eligibility of UASI not addressed should be directed to the appropriate DOLA/DEM Program Manager. All expenditures and items listed in the application must be allowable according to <http://www.ojp.usdoj.gov/odp/docs/fy2006hsgp.pdf>.

**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.

**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.

### ***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.

### **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 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 builds 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 predesignated temporary housing sites.

### **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.

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 closeout 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.***

**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		

**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

## **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.

## **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 10% 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.

## **Management and Administration**

Local jurisdiction subgrantees may retain and use up to 3 percent of their subaward from the State for local M&A purposes.

### ***UASI Target Capabilities***

- Planning
- Community Preparedness and Participation
- Communications
- Risk Management
- Information 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 & Agriculture 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 Information & 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 & Decontamination
- Structural Damage Assessment & Mitigation
- Economic & Community Recovery
- Restoration of Lifelines

## **XVII.2005 Citizen Corps Program (CCP)**

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.

### ***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:

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

### ***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.

Any questions concerning the eligibility of CCP not addressed should be directed to the appropriate DOLA/DEM Program Manager. All expenditures and items listed in the application must be allowable according to <http://www.ojp.usdoj.gov/odp/docs/fy2006hsgp.pdf>.

### **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.

### **Reporting Requirements**

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).

### ***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.

### **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 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, to have citizen advocates sit on existing advisory councils and task forces are 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 should 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 Colorado 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 Colorado 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.

**Organization**

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

**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**

<b>Cat. #</b>	<b>Category Title</b>	<b>Cat. #</b>	<b>Category Title</b>
[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

**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, 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.

### **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.

### **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 10% 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). 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.

### **Management and Administration**

Local jurisdiction subgrantees may retain and use up to 3 percent of their subaward from the State for local M&A purposes.

### ***CCP Target Capabilities***

- Community Preparedness and Participation  
*Citizen Preparedness and Participation Cuts Across:*
- Planning
- Communications
- Risk Management
- Information Gathering and Recognition of Indicators
- Law Enforcement Investigation and Operations
- Intelligence Analysis and Production
- CBRNE Detection
- Information Sharing
- Critical Infrastructure Protection
- Food & Agriculture 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

## **XVIII. Metropolitan Medical Response System (MMRS)**

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.

Any questions concerning the eligibility of MMRS not addressed should be directed to the appropriate DOLA/DEM Program Manager. All expenditures and items listed in the application must be allowable according to <http://www.ojp.usdoj.gov/odp/docs/fy2006hsgp.pdf>.

### ***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.

## **XIX. References**

Additional NIMS Info: <http://www.fema.gov/nims>

Authorized Equipment List: <http://www.rkb.mipt.org>

Blended Learning Strategies: <http://www.ojp.usdoj.gov/odp/training>

Develop New Training Courses: <http://www.ojp.usdoj.gov/odp/training.htm>

Exercise Info: <http://www.ojp.usdoj.gov/odp/exercises.htm> or <http://www.llis.gov>

Exercise Scheduler: <https://odp.esportals.com>

Homeland Security Presidential Directory HSPD-8:

<http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html>

Homeland Security Grant Program Training: <http://198.104.156.52/ODPWebforms/Index.asp>

Information Bulletin #132: <http://www.ojp.usdoj.gov/odp/docs/bulletins.htm>

Information Bulletin #180: <http://www.ojp.usdoj.gov/odp/docs/info180.pdf>

National Planning Scenarios and UTL Info: <https://odp.esportals.com>

NIMS Courses: <http://training.fema.gov/EMIWeb/IS/is700.asp>

ODP Announcement: <http://www.ojp.usdoj.gov/odp/docs/fy2006hsgp.pdf>.

ODP Prevention and Deterrence: <http://www.ojp.usdoj.gov/odp/docs/ODPPrev1.pdf>

Training Courses: <http://www.ojp.usdoj.gov/odp/docs/coursecatalog.pdf>

XML Information: <http://www.it.ojp.gov/gjxdm>

## TIME TABLE

01-05-2006	Program Capability Review of the 36 capabilities, AHEMR and the State must submit the completed reviews to CU
01-11-2006	Program Capability Review (10 <sup>th</sup> and 11 <sup>th</sup> )
02-06-2006	State, UASI, and Regional draft applications due (UASI must submit an investment justification and narrative for each initiative for 2006 funding)
03-02-2006	Colorado submits application to ODP for 2006 Homeland Security Funding
03-06-2006	Technical Assistance for state and regional applications
04-03-2006	Regional and State Departments FINAL applications due
05-08-2006	Regional Presentation of 2006 applications (8 <sup>th</sup> 9 <sup>th</sup> and 10 <sup>th</sup> )
06-15-2006	Grants awarded
07-01-2006	Grant Award Start Date

## CONTACTS

**Carmen Velasquez**  
[Carmen.Velasquez@state.co.us](mailto:Carmen.Velasquez@state.co.us)  
9195 East Mineral Avenue  
Centennial, CO 80112-3549

**DickVnuk**  
[Dick.Vnuck@state.co.us](mailto:Dick.Vnuck@state.co.us)  
9195 East Mineral Avenue  
Centennial, CO 80112-3549

**Judy Will**  
[Judy.Will@state.co.us](mailto:Judy.Will@state.co.us)  
9195 East Mineral Avenue  
Centennial, CO 80112-3549

**Randy Kennedy**  
[Randy.Kennedy@state.co.us](mailto:Randy.Kennedy@state.co.us)  
9195 East Mineral Avenue  
Centennial, CO 80112-3549

**Tony Reidell**  
[Tony.Reidell@state.co.us](mailto:Tony.Reidell@state.co.us)  
9195 East Mineral Avenue  
Centennial, CO 80112-3549

**Paul L. Cooke, Director**  
[Paul.Cooke@cdps.state.co.us](mailto:Paul.Cooke@cdps.state.co.us)  
9195 East Mineral Ave  
Centennial, CO 80112-3549