U. S. Department of Homeland Security

Office for Domestic Preparedness

Washington, D.C. 20531

ODP Information Bulletin
No. 84 October 1, 2003

TO: All State Administrative Agency Heads
All State Administrative Agency Points of Contact

FROM: Andrew T. Mitchell
Acting Director

SUBJECT: Critical Infrastructure Protection Funds

The Office for Domestic Preparedness (ODP), Department of Homeland Security (DHS) has reviewed the list of categories eligible for funding with FY03 supplemental Critical Infrastructure Protection (CIP) funds. Based upon this review, ODP has determined that additional activities and expenses are allowable with these funds. In addition to original guidance provided in the FY03 State Homeland Security Grant Program (SHSGP) - Part II and the Urban Areas Security Initiative (UASI) - Part II application kits, the following categories of activities and expenses may now also be financed with CIP funds:

- Equipment for CIP target hardening and Preventive Security Enhancements
- Assessments of critical infrastructure sites (e.g., vulnerability assessments; security force requirements; CIP cost assessments)
- Related critical infrastructure terrorism prevention activities
- CIP Protective Security Exercises and Training
- Development of Community Based Security Buffer Zone Plans

This expansion of allowable activities and expenses is effective immediately for SHSGP - Part II and UASI - Part II. Allowable expenses may be reimbursed for obligations that occurred on or after the grant project period start date. Below we have provided guidance on these expanded categories. Prior to obligation or expenditure of funds, grantees must provide detailed budget worksheets to their ODP Program Manager for review and approval. Requests for reimbursement of existing obligations should also be made to the appropriate ODP Program Manager for review and approval prior to draw-down of funds.

Critical Infrastructure Sites:

As noted in the SHSGP- Part II and UASI- Part II grant application kits, critical infrastructure includes any system or asset that if attacked would result in catastrophic loss of life/or catastrophic economic loss. In addition, protection for the following specific types of facilities should also be considered:

- Public water systems serving large population centers
- Primary data storage and processing facilities, major stock exchanges and major banking centers
- Chemical facilities located in close proximity to large population centers
- Major power generation facilities that exceed 2000MW and if successfully attacked would disrupt the regional electric grid
- Hydroelectric facilities and dams that produce power in excess of 2000MW or could result in catastrophic loss of life if breached
- Nuclear power plants
- Electric substations 500KV or larger, and substations 345 KV or larger that are part of a critical system supporting populations in excess of one million people
- Rail and highway bridges over major waterways that, if destroyed, would cause catastrophic loss of life or catastrophic economic impact
- Major natural gas transmission pipelines in excess of 3000 bcf throughput
- Natural Gas and liquid Natural Gas Storage (LNG) facilities
- Major petroleum handling facilities such as pipelines, ports, refineries and terminals
- Major mass transit subway systems and the supporting ventilation systems
- Telecommunications, internet, and cyber facilities

Note: protective security enhancements for large public gatherings/areas such as sporting events, outdoor concerts, are considered to be included under the criteria above.

Expanded categories eligible with CIP funds:

Equipment for CIP Target Hardening and Preventing Attacks

Equipment designed to enhance the physical security of critical infrastructure is also allowable. This equipment will either prevent and/or deter an attack or will mitigate the effects of an attack.

Surveillance, Warning, Access/Intrusion Control

- Ground Systems: Motion detection Systems, barriers, impact resistant doors, portal and locking systems, alarm systems, video assessment/Cameras, personnel identification systems, access control devices, X-Ray units, magnetometers, vehicle identification systems

- Waterfront Systems: Radar systems, video assessment System/Cameras, diver/swimmer detection systems, sonar, impact resistant doors, portal systems hull scanning equipment, Ground/Wall penetrating radar

Sensors- Agent/Explosives Detection

- Chemical
- Biological
- Radiological
- Nuclear
- Explosive

Inspection/Detection Systems

- Vehicle and cargo inspection systems (Gamma-ray)
- Mobile Search & Inspection system (X-Ray)
- Non-invasive CBRNE system (Pulsed neutron activation)

Explosive Protection

- Blast/shock/Impact resistant systems
- Protective clothing
- Column and surface wraps; Breakage/shatter resistant glass; Window traps
- Robotic disarm.disable systems

Terrorism Incident Prevention equipment (Terrorism Early warning prevention and deterrence technology and equipment)

- Data collection/information gathering software
- Data synthesis software
- Geographic information system technology and software
- Law enforcement surveillance equipment

Assessments of Critical Infrastructure Sites

Assessments of the CIP sites can assist in determining specific vulnerabilities, equipment and/or personnel required to protect and secure sites, and resources (financial, personnel, etc.) required for security enhancements/deployments. Examples of allowable assessments include:

- vulnerability assessments

- security equipment/force requirements
- CIP cost assessments

Related Critical Infrastructure terrorism prevention activities

Examples of other terrorist prevention activities include: planning, public information/education programs and neighborhood watch activities.

- Planning for enhancing security during heightened alerts, during terrorist incidents, and/or during mitigation and recovery
- Public information/education: printed and electronic materials, public service announcements, seminars/town hall meetings, web postings
- Neighborhood watch activities in communities surrounding CIP sites

CIP Exercises

CIP exercises must be conducted in accordance with the Homeland Security Exercise and Evaluation Program (HSEEP). seminars, tabletop exercises, drills, functional exercises and full-scale exercises. are all allowable activities. The exercise scenario should test: plans,protective/preventative measures that have been instituted or are in development, and response activities. Examples of exercise scenarios include:

- A seminar addressing vulnerabilities of specific sites (such as a power grid, gas plant, or chemical plant) to terrorist attack
- A seminar focusing on roles and responsibilities of on-site personnel and/or specially deployed security personnel during heightened states of alert
- A tabletop exercise focusing on deployment of security/protection resources (Law Enforcement, National Guard, etc)
- A tabletop exercise involving a deliberate attack on a critical infrastructure site focusing on infrastructure security/protection activities before, during and/or after an incident
- A full-scale exercise involving an attack on a critical infrastructure site that includes appropriate integration of security/protective personnel in the exercise scenario

CIP Training

CIP training must be designed to enhance the capabilities to protect and secure critical infrastructure. This program may be institutionalized within existing training academies, at the CIP site or at another appropriate location. Target audiences for the training include facility managers, facility personnel, emergency managers, emergency responders and public/elected officials within the following disciplines: firefighters law enforcement, emergency management, emergency medical services, hazardous materials, public works, public health, health care, public safety communications, governmental administrative, private security guards and on-site response personnel, and support and managerial staff. Training programs should be appropriate for both the level (Awareness, Performance, Planning/Management) and discipline (Fire, Law Enforcement, Emergency Management, Public Health, Healthcare, etc) of the participant, and must be consistent with current State and local guidelines. Where applicable, training should also follow ODP training doctrine to include Emergency Responder Guidelines providing an integrated compilation of responder skills, knowledge, and capabilities which fosters interoperability and an understanding of how all of the elements of a response fit together.

Examples of allowable training include:

- Inticators of terrorist activity in the vicinity of critical infrastructure (Indications and Warnings)
- Terrorism Prevention training tailored to the operational environment.
- CBRNE Awareness Training for personnel employed at critical infrastructure sites
- Training on the roles/responsibilities of Law Enforcement, National Guard or other security personnel that may be deployed to critical infrastructure sites
- Site specific training (for familiarization of sites) for personnel that currently provide security or may be deployed to the critical infrastructure sites

For more information on CIP funding, please contact your ODP Program Manager by calling the ODP Helpline at (800) 368-6498.