U.S. Department of Homeland Security

Fiscal Year 2005 Buffer Zone Protection Program

Program Guidelines and Application Kit

U.S. Department of Homeland Security

U.S. Department of Homeland Security

Office of State and Local Government Coordination and Preparedness

Office for Domestic Preparedness

In Coordination With

Information Analysis and Infrastructure Protection Directorate

Protective Security Division

Disclaimer

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

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

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

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

FOREWORD

On October 18, 2004, the President signed the Fiscal Year 2005 Homeland Security Appropriations Act, thereby providing vital funding needed to ensure the safety and security of our homeland. Through a partnership between the Office for Domestic Preparedness (ODP) and the Information Analysis and Infrastructure Protection (IAIP) Directorate, the Department of Homeland Security (DHS) will provide protective action funding to protect and secure critical infrastructure and key resource (CI/KR) sites across the country. This infrastructure protection funding represents a significant commitment by Congress to better secure America against the threat posed by terrorism.

The Buffer Zone Protection Program (BZPP) is designed to reduce vulnerabilities of CI/KR sites by extending the protected area around a site into the surrounding community and supporting the prevention and preparedness efforts of local first responders. The FY 2005 BZPP grants will provide funding for the equipment and management of these protective actions at CI/KR sites across the country, so that we can better safeguard our nation and minimize the potential for terrorist attacks.

The BZPP reflects the Department's commitment to work closely with the nation's prevention, preparedness and response communities and the private sector in a unified national effort to combat terrorism and secure our homeland.

Michael Chertoff
Secretary
Department of Homeland Security

Contents

I. Eligible Applicants and Funding Availability 1
II. Application Kit 5
III. Buffer Zone Protection Program Overview and Guidance 9
IV. Award and Reporting Requirements 30

Appendix A	Sample Award Package
Appendix B	Guidance for Development of Interoperable Communications Plans
Appendix C	List of Terms

I. ELIGIBLE APPLICANTS AND FUNDING AVAILABILITY

FY05 BZPP funding should be coordinated with FY05 Homeland Security Grant Program (HSGP) funding, where applicable, to leverage additional funding, resources, and to achieve goals and objectives outlined in State and/or Urban Area Homeland Security Strategies. Specifically, FY05 BZPP activities should be coordinated with FY05 HSGP - Law Enforcement Terrorism Prevention Program (LETPP) Target Hardening activities, to avoid duplication of funding efforts and to support ongoing CI/KR protection and preparedness efforts.

The LETPP seeks to provide law enforcement communities with enhanced capabilities for detecting, deterring, disrupting, and preventing acts of terrorism. The FY05 LETPP provides communities with funds for the following activities: 1) information sharing to preempt terrorist attacks; 2) **target hardening to reduce vulnerability of selected high value targets** (*see below*); 3) threat recognition and mapping of potential or developing threats; 4) intervention activities to interdict terrorists before they can execute a threat; and 5) interoperable communications.

- **Target Hardening to Reduce Vulnerability**: Funds provided under this category of the LETPP allow communities to make vulnerable targets more resistant to attack or more difficult to destroy or damage. Allowable use of funds includes the development of related critical infrastructure terrorism prevention activities such as:

  - Planning for enhanced security during HSAS 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
  - Evaluating Critical Infrastructure Protection (CIP) security equipment and/or personnel requirements to protect and secure sites
  - CIP cost assessments, including resources (financial, personnel, etc.) required for security enhancements/ deployments

Drawdown of Funds

Grantees and subgrantees will be permitted to drawdown funds up to ***120*** days prior to expenditure/disbursement, which echoes the recommendation of the Funding Task Force. However, DHS must provide written approval of the completed BZP and VRPP for each site before FY05 BZPP funds may be obligated, drawn down, or expended by the state to the responsible jurisdiction of that site. Funds received by both grantees and subgrantees must be placed in an interest-bearing account and are subject to the rules outlined in the Uniform Rule 28 CFR Part 66, *Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments*, at http://www.access.gpo.gov/nara/cfr/waisidx_04/28cfrv2_04.html and the Uniform Rule 28 CFR Part 70, *Uniform Administrative Requirements for Grants and Agreements (Including Subawards) with Institutions of Higher Education, Hospitals, and other Nonprofit Organizations*, at

http://www.access.gpo.gov/nara/cfr/waisidx_03/28cfr70_03.html. These guidelines state that subgrantees are required to promptly, but at least quarterly, remit interest earned on advances to:

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

The grantee or subgrantee may retain interest amounts up to $100 per year for administrative expenses. Please consult the *Office of Justice Programs* (*OJP) Financial Guide* or the applicable OMB Circular for additional guidance.

State grantees are subject to the interest requirements of the Cash Management Improvement Act (CMIA) and its implementing regulations at 31 CFR Part 205. Interest under CMIA will accrue from the time federal funds are credited to a state account until the time the state pays out the funds to a subgrantee or otherwise for program purposes.

Federal Fiscal Oversight and Support

The OJP Office of the Comptroller (OC) will continue to provide fiscal support and oversight of the grant programs included in this solicitation. All grantees and subgrantees should refer to the *OJP Financial Guide*, available at http://www.ojp.usdoj.gov/FinGuide/. DHS will be establishing its own Office of Grant Operations (OGO) within ODP during FY05 and details on the transition of fiscal support and oversight of the grant programs will be forthcoming.

Freedom of Information Act (FOIA)

ODP recognizes that much of the information submitted in the course of applying for funding under this program, or provided in the course of its grant management activities, may be considered law enforcement sensitive or otherwise important to national security interests. This may include threat, risk, and needs assessment information, and discussions of demographics, transportation, public works, and industrial and public health infrastructures. While this information under federal control is subject to requests made pursuant to the Freedom of Information Act, 5. U.S.C. §552, all determinations concerning the release of information of this nature are made on a case-by-case basis by the DHS FOIA Office, and may likely fall within one or more of the available exemptions under the Act.

Additionally, information related to critical infrastructure protection that is submitted to DHS should bear the following statement: "This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002."

Applicants are encouraged to consult their own state and local laws and regulations regarding the release of information, which should be considered when reporting sensitive matters in the grant application, needs assessment and strategic planning process. Applicants may also consult their ODP Preparedness Officer regarding concerns or questions about the release of information under state and local laws.

Services to Limited English Proficient (LEP) Persons

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

D. FY 2005 BZPP Requirements

The following steps must be completed for each identified site before grant funds for the FY05 BZPP may be obligated, drawn down, or expended by the state to the responsible jurisdiction for that site.

BZPP Checklist

- □ **Responsible jurisdictions conduct vulnerability assessment or use existing assessment, if appropriate**
  - □ Coordinate with security management and measures already in place at the facility
- □ **Responsible jurisdictions use template and process to develop a BZP and VRPP for identified sites**
- □ **Responsible jurisdictions must coordinate the development of the BZP and VRPP with:**
  - □ Urban Area Working Groups, if applicable
  - □ Urban Area Homeland Security Strategies, if applicable
- □ **Upon completion, responsible jurisdictions must submit the BZP and VRPP to the SAA for:**
  - □ Coordination of the BZPP with State Homeland Security Strategies and programs
  - □ Coordination with related funding programs
- □ **SAA submits completed BZP and VRPP to DHS for review**
- □ **Upon approval, drawdown and expend funds to implement BZP**

Site Vulnerability Assessment

- A vulnerability assessment is a critical element of the BZPP process. Responsible jurisdictions are expected to conduct a vulnerability assessment of the specific infrastructure site, including the zone outside the perimeter of the potential target. It must include coordination with security management and measures already in place at the facility.

- The responsible jurisdictions are required to share these assessments with DHS upon request, so that DHS may better prioritize protective programs in the light of emerging and specific threats.

- DHS will then make the BZP template available to the SAA, who is expected to provide it to any local authority that requests it. The template should also be made available to local jurisdictions that are not responsible for CI/KR sites identified by DHS as being eligible for grant funding. The BZP template serves as a useful tool that can be integrated into any infrastructure protection program.

BZP Development, Review, and Approval

- Using the BZP template and process provided by DHS, responsible jurisdictions will develop a BZP in coordination with the state for each identified CI/KR site. This plan will become the basis to identify the required training, information, equipment, resources and recommended buffer zone protective measures necessary to address any shortfalls.

- Additionally, a VRPP must be completed. The VRPP identifies a spending plan, including the materials, equipment, and resources necessary to implement the BZP.

    - The BZP and VRPP should be provided to the SAA, to coordinate BZPP implementation with existing State and/or Urban Area Homeland Security Strategy goals and objectives, and with related HSGP funding.

- The SAA must submit the completed BZP and VRPP to DHS for review and approval.

    - The SAA must also provide written concurrence in support of the BZP and VRPP, between the state and responsible jurisdiction for each selected CI/KR site to DHS.

- The SAA must submit the BZP and VRPP on CD via *Overnight Mail* to ODP at:

  Office for Domestic Preparedness
  Attn: CSID - BZPP
  810 7th Street, NW
  Washington D.C., 20531

  Phone Number: 1-800-368-6498

  The CD must include a label with the following information:
  - State
  - Identified CI/KR Site, and
  - Responsible Jurisdiction (subgrantee)

- The SAA must also email their respective ODP PO (and carbon copy the BZPP@dhs.gov email address) with the above information, along with the overnight mail tracking number, on the day the CD containing the BZP and VRPP was mailed.

- ***Note:*** *All email correspondence, between the grantee and DHS, related to the application, submission, approval, and/or revision of BZPs and VRPPs must carbon copy the BZPP@dhs.gov email address. This will assist and support DHS with the logging, tracking, and related reporting requirements for the BZPP.* ***However, the actual BZPs and VRPPs should never be sent via email.***

- Upon review and approval of the BZP and VRPP by DHS, the responsible jurisdiction(s) may drawdown and expend grant funds obligated by the SAA for implementation of the BZP.

Funds under the FY05 BZPP may not be obligated, drawn down, or expended by the state to the responsible jurisdiction of the identified site until all of the above steps have been completed and approval has been granted by DHS for each site.

E. Allowable Costs Guidance

States, urban areas, and local jurisdictions should leverage existing ODP HSGP funds, including the State Homeland Security Program (SHSP), Urban Areas Security Initiative (UASI), and the LETPP, for any activities related to the planning, development and organization of FY05 BZPP activities and according to their stipulated authorized expenditures. This includes funds for conducting the vulnerability assessment and related BZP training and exercise activities.

Funding from the FY05 BZPP should be reserved for the acquisition and use of the allowable materials, equipment, and resources identified in the VRPP, as necessary, to implement protective measures that will reduce vulnerabilities around identified CI/KR sites. A limited amount of FY05 BZPP funding may be used to support M&A activities directly related to FY05 BZPP development and implementation.

Additionally, any resulting training or exercise requirements identified in the BZPP may not be funded with FY05 BZPP funds, but may be funded with SHSP, UASI, and/or LETPP funds, and in accordance with their stipulated authorized expenditures.

This section serves as a guide for program expenditure information for the FY05 BZPP. Grantees are encouraged to contact their ODP Preparedness Officer regarding authorized and unauthorized expenditures.

Funding may only be used in the following categories:

1. Equipment Acquisitions; and,
2. Management and Administrative (M&A).

Equipment

FY05 BZPP funds may be used for equipment acquisition from equipment categories (see *Suggested AEL Categories* on page 19) listed in the FY05 ODP Authorized Equipment List (AEL), which is housed on the web-based Responder Knowledge Base (RKB). BZPs are intended to encourage creative solutions to mitigate vulnerabilities. **Therefore, VRPPs that include requests for equipment in the AEL, but not in the suggested equipment categories included on page 20, will be reviewed by DHS for approval on a case-by-case basis.** However, all equipment must be included in the VRPP and the VRPP must be submitted and approved by DHS prior to the drawdown or use of any FY05 BZPP funds.

Federal grant money cannot be used for the improvement of Federal buildings or for other activities that solely benefit the Federal government. In the case of Federal BZPP sites, the grantees can work to improve the perimeter, but cannot improve the actual building, i.e., they cannot install cameras and fences that would, in the end, be Federal property.

The RKB is sponsored by ODP and the Oklahoma City National Memorial Institute for the Prevention of Terrorism (MIPT) and is located at http://www.rkb.mipt.org. The website is designed to provide emergency responders, purchasers, and planners with a trusted, integrated, online source of information on products, standards, certifications, grants, and other equipment related information. By integrating this information, which includes the InterAgency Board's (IAB) Standardized Equipment List (SEL) and the AEL from ODP, into one location, responders, vendors, standards organizations, training facilities, and grant making organizations have a trusted first source to answering questions such as:

- What equipment is on the market?
- Has it been certified?
- If so, to what standard?
- What training is needed to use it effectively?
- Are there experts available for consultation and questions?

The FY05 ODP AEL is housed on the RKB and relies heavily on the SEL developed by the IAB for Equipment Standardization and Interoperability. The 2005 AEL has been modified to facilitate cross-referencing of the SEL in an effort to eliminate redundancy. Both the AEL and SEL are available on the RKB, which also offers an interactive version that provides links to corresponding SEL items and commercial products.

In some cases, items on the SEL are not allowable under FY05 BZPP or will not be eligible for purchase unless specific conditions are met. In addition, some items eligible under this grant program are beyond the scope of the SEL and thus will only appear in the AEL.

If state agencies and/or local governments have questions concerning the eligibility of equipment not specifically addressed in the AEL, they should contact their ODP Preparedness Officer for clarification.

The suggested AEL categories for the FY05 BZPP are listed in the table below.

Suggested AEL Categories

AEL Category	Category Title

2	**Explosive Device Mitigation and Remediation Equipment**
	• Protective Equipment
	• Mitigation and Remediation Equipment
	  o Kit, Fiber Optic
	  o Detector, Metal
	  o Robot, Attachments, Tools
	  o Robot Upgrades
	  o Tools, Remote Opening, Examination, Related Equipment
	  o X-Ray Unit, Portable or Transportable
	  o Tools, IED Remediation, Non-Explosive
	  o Tools, Pipe Bomb Disabling

6	**Interoperable Communications Equipment** • In-Suit Communications • Radio, Portable/Mobile/Base/High Frequency (HF) Single Sideband • Repeaters • Transmission Device, Wireless, Remote Sensor • Cable, Non-radiation Shielded Transmission • Amplifiers, Bi-directional • Bridging/Patching • Exchange, Private Branch • Phone, Cellular • Device, Messaging, 2-Way Text • Paging • Phone, Satellite Base • Radio, Microwave Link • Phone, Satellite Mobile/Portable • Services, Satellite, Brokered • Services, Satellite Data • INMARSAT - B • Hourly Brokered Space Segment • Full Time Space Segment, Leased • Equipment, Satellite Data • Network, Wide Area Digital • Device, Data Service Access • Teleconferencing, Video • Bridge, Audio Teleconferencing • Bridge, Video Teleconferencing • Computer-Aided Dispatch • Mobile Display Terminals • Antenna and Tower Systems • Communications Priority Services • Aviation and Maritime Security Voice and Data Transmission

AEL Category	Category Title
	• Safe, GSA-Rated • Shredder / Disintegrator • System, Automated Dialing and Notification • Systems, Public Notification and Warning

7	**Detection Equipment**
	• Biological
	  o Biological Detection
	  o Biological Sampling
	• Chemical
	  o Chemical Detection
	  o Chemical Sampling
	• Radiological/Nuclear
	  o Radiological Detection
	  o Radiological Sampling
	• Explosive Detection
	  o Handheld Air-Sampler, Explosive Detecting
	  o Swipe Test, Explosive Detecting
	  o Portal, Explosive Detecting
	  o X-Ray, Explosive Detecting
	• Other Detection / Sensor Equipment
	• Equipment, Environmental (Weather) Surveillance
	• Sensor, Heat, Infrared
	• Thermometer, Surface
	• Protective Cases for Sensitive Detection Equipment - Storage

14	**Physical Security Enhancement**
	• Surveillance, Warning, Access/ Intrusion Control
	  o General
	  ▪ Systems, Motion Detection
	  ▪ Barriers: Fences; Jersey Walls
	  ▪ Doors and Gates, Impact Resistant
	  ▪ Portal Systems; locking devices for access control
	  ▪ Systems, Alarm
	  ▪ Video Assessment
	  ▪ Systems, Personnel Identification
	  ▪ Systems, Vehicle Identification
	  ▪ X-Ray Units
	  ▪ Magnetometers
	  o Waterfront
	  ▪ Systems, Radar
	  ▪ System, Diver/Swimmer Detection; Sonar
	  ▪ Equipment, Hull Scanning
	  ▪ Barriers, Vessel
	• Explosion Protection

AEL Category	Category Title
	o Systems, Blast/Shock/Impact Resistant o Wraps, Column and Surface; Breakage/Shatter Resistant Glass o Trash Receptacles, Bomb-Resistant • Support Equipment for Continuation of Critical Infrastructure Operations o Fuel storage containers o Sensors and Alarms, Self-Monitoring o Back-up operating computer hardware and programming software
15	**Inspection and Screening Systems** • System, Vehicle & Cargo Inspection; Gamma-Ray • System, Mobile Search & Inspection; X-ray • System, Non-Invasive, Radiological/ Chem/ Bio/ Explosives • Radar, Ground/Wall Penetrating • Monitors, Portal

Management and Administrative Costs

No more than **3% of the total amount** allocated to the state for the BZPP may be retained at the state level and used for M&A purposes related to the FY05 BZPP. These state M&A funds must be included in the total funds retained by the state. In addition, responsible jurisdiction subgrantees may retain and use up to ***2.5% of their subaward*** from the state for local M&A purposes. States may pass through a portion of the state M&A allocation to subgrantees in order to supplement the 2.5% M&A allocation allowed on subgrants. However, no more than 3% of the total subaward may be expended by subgrantees on M&A costs.

The following are allowable M&A costs:

Allowable M&A Costs
• **Hiring of full-time or part-time staff or contractors/consultants**: o To assist with the management of the FY05 BZPP. o To assist with equipment design, requirements, and implementation of the FY05 BZPP.

Allowable M&A Costs

- **Hiring of full-time or part-time staff or contractors/consultants and expenses related to**:
  - Meeting compliance with reporting and data collection requirements, including data call requests.
  - FY05 BZPP pre-application submission management activities and application requirements.

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

- **Travel expenses**

- **Meeting-related expenses** (For a complete list of allowable meeting-related expenses, please review the OJP OC Financial Guide at http://www.ojp.usdoj.gov/FinGuide).

- **The following are allowable only within the period of performance of the grant program**:
  - Acquisition of authorized office equipment, including personal computers, laptop computers, printers, LCD projectors, and other equipment or software which may be required to support the implementation of the homeland security strategy.
  - Recurring fees/charges associated with certain equipment, such as cell phones, faxes, etc.
  - Leasing and/or renting of space for newly hired personnel to administer the FY05 BZPP.

Construction and Renovation

The use of FY05 BZPP funds for construction or renovation, as well as the following activities, is allowable only when it is a necessary component of a security system or target hardening activity at CI/KR sites.

- The following actions and improvements do not constitute construction or renovation, and are allowable under FY05 BZPP guidance:
  - Improved lighting
  - Fencing
  - Closed-circuit television (CCTV) systems
  - Motion detection systems
  - Barriers, doors, gates and related security enhancements.

- Project construction and renovation is allowable under the FY05 BZPP. Funds may be used for construction and renovation projects ***only*** when those projects specifically address ***enhanced security or target hardening activities at critical infrastructure facilities***. The following actions and improvements are considered to constitute construction or renovation, and justification for this construction and/or renovation must be addressed in the VRPP. The VRPP must be submitted to the SAA and approved by DHS.
  - Construction and/or renovation to guard facilities
  - Communications antennas
  - Any other construction or renovation efforts that change or expand the footprint of a facility or structure, including security enhancements to improve perimeter security.

- **Justification and Approval Process**. Grantees and/or subgrantees must provide the following justification information in the VRPP for any construction and/or renovation activities necessary to implement the BZP.

  The grantee must provide to DHS:
  - Description of the asset or facility, asset location, whether the infrastructure is publicly or privately owned, and the construction or renovation project
  - Certification that a facility vulnerability assessment has been conducted for the facility
  - How the construction or renovation project will address the identified vulnerability(ies) from the assessment
  - Consequences of not implementing the construction or renovation project

- The justification for these expenditures (as outlined above) must be addressed in the VRPP, and the VRPP must be **submitted and approved by DHS** prior to the drawdown or use of any FY05 BZPP funds for construction or renovation.

- **National Environmental Policy Act (NEPA)**: NEPA requires DHS to analyze the possible environmental impacts of each construction project. The purpose of a NEPA review is to weigh the impact of major federal actions or actions undertaken using federal funds on adjacent communities, water supplies, historical buildings, endangered species, or culturally sensitive areas prior to construction. Grantees wishing to use DHS funding for construction projects must complete and submit a **NEPA Compliance Checklist** to their respective ODP Preparedness Officer for review. Additionally, grantees may be required to provide additional detailed information on the activities to be conducted, locations, sites, possible construction activities, possible alternatives, and any environmental concerns that may exist. Results of the NEPA Compliance Review could result in a project not being approved for DHS funding, the need to perform an Environmental Assessment (EA) or draft an Environmental Impact Statement (EIS).

F. Unallowable Costs Guidance

Unauthorized program expenditures for all programs under the FY05 BZPP include:

- Hiring of full or part-time public safety personnel for the purposes of fulfilling traditional public safety activities;
- Expenditures for items such as general-use software (word processing, spreadsheet, graphics, etc), general-use computers and related equipment (other than for allowable M&A activities, or otherwise associated preparedness or response functions), general-use vehicles, licensing fees, weapons systems and ammunition;
- Funds used for the improvement of Federal buildings or for other activities that solely benefit the Federal government;
- Activities unrelated to the completion and implementation of the BZP; and,
- Other items not in accordance with the AEL or previously identified within this guidance as an allowable cost.

G. DHS Resources and Support

To assist grantees with program activities, ODP and IAIP have several support mechanisms available to grantees.

PSD Protective Measures Section

PSD Protective Measures Section will provide a range of services to BZPP grantees and subgrantee. This includes BZPP workshops to further explain the BZPP and process, and additional guidance in developing VRPPs. PSD also

provides on-site technical assistance for officials needing additional technical support in developing and/or implementing BZPs. PSD will also serve as the primary point of contact for state and local homeland security officials regarding questions, concerns, planning, general issues, and accessing specialized experience for the overall program.

For additional information on BZPP workshops and on-site technical assistance to support the development and implementation of BZPs, please contact the PSD Protective Measures Section Chief, Bill Eagan, at 202-282-8737.

Role of ODP's Preparedness Officers

Throughout the project period, ODP Preparedness Officers will work closely with state and local officials to assist agencies in enhancing their homeland security preparedness through planning, training, equipment acquisition, exercises, and technical assistance. Preparedness Officers will be in continuous contact with the SAAs and local officials, and should be considered as the point of contact within ODP for addressing questions, concerns, general issues, and accessing specialized experience. Please contact your state SAA or the ODP helpline at 800-368-6498 to identify and contact your ODP Preparedness Officer.

Centralized Scheduling and Information Desk (CSID) Help Line

CSID is a non-emergency resource for use by state and local emergency responders across the nation. CSID provides general information on all ODP programs and information on the characteristics and control of CBRNE materials, defensive equipment, mitigation techniques, and available federal assets and resources. CSID also provides information on the following services: CBRNE training, centralized scheduling capability, CBRNE exercises, State Homeland Security Assessment and Strategy Grants, and technical assistance (TA).

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

Homeland Security Preparedness Technical Assistance Program (HSPTAP)

ODP's technical assistance program provides direct assistance to state and local jurisdictions to improve their ability to prevent, respond to, and recover from threats or acts of terrorism involving CBRNE weapons. A primary objective of the program is to enhance the capacity of state and local jurisdictions, as well as special needs jurisdictions such as port authorities and mass transit agencies to develop, plan, and implement effective strategies for CBRNE preparedness. TA may be provided to state and local governments, law enforcement, fire,

hazardous materials, and other community agencies that have CBRNE responsibilities, including Citizen Corps Councils. *All TA services are available to eligible recipients at no charge. ODP will cover the cost of providing the technical expertise, travel, and related expenses.*

- **National Criminal Justice Association (NCJA).** NCJA is the HSPTAP provider for the TA service entitled *Enhancing Grants Management Capacities*, which seeks to further improve the ability of SAAs to manage and account for grant funds awarded by ODP.

- **Domestic Preparedness Equipment Technical Assistance Program (DPETAP**). DPETAP provides on-site training in the selection, use, and maintenance of specialized CBRNE detection and response equipment by providing detailed technical information, hands-on equipment operation, and maintenance training.

Additional information on HSPTAP can be found online at ODP's TA website at www.ojp.usdoj.gov/odp/ta.htm under the *Catalog* link, or by contacting the CSID helpline at 800-368-6498.

Lessons Learned Information Sharing (LLIS) System

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

The system houses a directory of responders and homeland security officials, as well as an updated list of homeland security exercises, events, and conferences. Additionally, the LLIS includes online collaboration tools, such as secure email and message boards, where users can exchange information. LLIS uses strong encryption and active site monitoring to protect all information housed on the system.

ODP Applicant Assistance Services

Applicant Assistance Services are designed to provide grantees with assistance in completing and submitting their applications to meet the required deadlines. For more information concerning the suite of Applicant Assistance Services, please contact your ODP Preparedness Officer.

Equipment Purchase Assistance Program

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

Additional information on each of these programs can be found on the ODP web site located at http://www.ojp.usdoj.gov/odp or by contacting the state's assigned ODP Preparedness Officer through the ODP helpline at 800-368-6498.

IV. AWARD AND REPORTING REQUIREMENTS

IV. Award and Reporting Requirements

A. Grant Award to State

Upon approval of the application the grant will be awarded to the respective SAA. This date will be known as the "*award date*."

Required Submissions: Signed award document and special conditions returned to the OJP OC.

B. Drawdown and Expenditure of Funds

Following the grant award, completion of all grant award requirements, and release of any special conditions (i.e. completion of the vulnerability assessment and approval of the BZP and VRPP), the grantee can drawdown and expend grant funds through the electronic PAPRS or LOCES systems. Drawdowns and expenditures must be reported to ODP on a quarterly basis through the Financial Status Reports (FSR), which are due within 45 days of the end of each calendar quarter (i.e. for the quarter ending March 31, FSR is due on May 15). A report must be submitted for every quarter the award is active, including partial calendar quarters, as well as for periods when no grant activity occurs. OJP OC will provide a copy of this form in the initial award package. Future awards and fund drawdowns will be withheld if these reports are delinquent.

In support of our continuing effort to meet the accelerated financial statement reporting requirements mandated by the U. S. Department of the Treasury and the Office of Management and Budget (OMB), payment processing will be interrupted during the last five (5) working days each month. Grantees/contractors should make payment requests before the last five working days of the month to avoid delays in deposit of payments.

For example, for the month of January, the last day to request (drawdown) payments will be January 23, 2005. Payments requested after January 23, 2005 will be processed when the regular schedule resumes on February 2, 2005. A similar schedule will follow at the end of each month thereafter.

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

Questions regarding grant accounts should be addressed to the OJP OC at 1-800-458-0786 or e-mail askoc@ojp.usdoj.gov.

Required Submissions: SF-269 FSR (quarterly)

C. Reporting Requirements

Reporting requirements for the FY05 BZPP are consolidated in a single reporting system to minimize the administrative burden on states. While budget detail worksheets do not need to be submitted as a requirement of the initial grant application, procurement plans must be approved prior to obligation, drawdown or expenditure of funds. Additionally, the representative states also must maintain complete and accurate accounting records, and must make those records available to DHS upon request.

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

- 28 CFR Part 66, *Uniform administrative requirements for grants and cooperative agreements to state and local governments*, at http://www.access.gpo.gov/nara/cfr/waisidx_04/28cfrv2_04.html
- OMB Circular A-87, *Cost Principles for State, Local, and Indian Tribal Governments,* at http://www.whitehouse.gov/omb/circulars/index.html
- 28 CFR Part 70, *Uniform administrative requirements for grants and agreements (including subawards) with institutions of higher education, hospitals and other nonprofit organizations*, at http://www.access.gpo.gov/nara/cfr/waisidx_04/28cfrv2_04.html
- OMB Circular A-21, *Cost Principles for Educational Institutions,* at http://www.whitehouse.gov/omb/circulars/index.html
- OMB Circular A-122, *Cost Principles for Non-Profit Organizations,* at http://www.whitehouse.gov/omb/circulars/index.html.

Additionally, grantees should be familiar with the requirements included in OJP's OC *Financial Guide* at http://www.ojp.usdoj.gov/FinGuide/.

Required Submissions: FSR (quarterly).

Financial and Compliance Audit Report

Recipients that expend $500,000 or more of federal funds during the fiscal year are required to submit an organization-wide financial and compliance audit report. The audit must be performed in accordance with the U.S. General Accounting Office *Government Auditing Standards*, located at http://www.gao.gov/govaud/ybk01.htm, and *OMB Circular A-133*, *Audits of*

States, Local Governments, and Non-Profit Organizations, located at http://www.whitehouse.gov/omb/circulars/index.html. Audit reports are currently due to the Federal Audit Clearinghouse no later than 9 months after the end of the recipient's fiscal year. In addition, the Secretary of Homeland Security and the Comptroller General of the United States shall have access to any books, documents, and records of recipients of FY05 BZPP assistance for audit and examination purposes, provided that, in the opinion of the Secretary of Homeland Security or the Comptroller General, these documents are related to the receipt or use of such assistance. The grantee will also give the sponsoring agency or the Comptroller General, through any authorized representative, access to and the right to examine all records, books, papers or documents related to the grant.

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

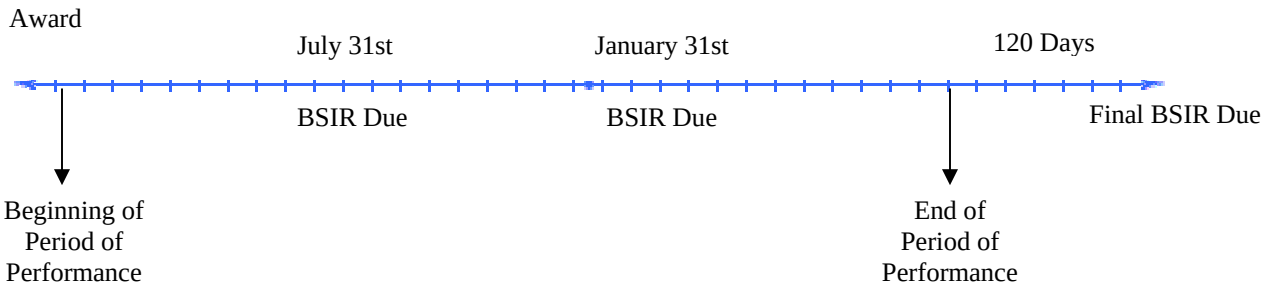
Biannual Strategy Implementation Report (BSIR)

ODP has launched a web application for states' submissions of the BSIR. The BSIR is designed to outline how state, urban area, and local ODP grant funding is being used to meet the strategic goals and objectives outlined in the State and Urban Area Homeland Security Strategies. All BSIR submissions must be submitted online via the Grants Reporting Tool (GRT) and it must be completed by state grantees and subgrantees at the state, urban area, and local levels. The GRT can be accessed at https://www.reporting.odp.dhs.gov/.

Following award of the grant, the state and subgrantees will be responsible for providing updated obligation and expenditure information on a regular basis. The BSIR submission will satisfy the narrative requirement in Box 12 of the biannual Categorical Assistance Progress Report (CAPR). States will still be required to submit the CAPR form. The BSIR is due within 30 days after the end of the reporting period (July 31 with a reporting period of January 1 through June 30, and on January 31 with a reporting period of July 1 through December 31). Updated obligation and expenditure information must be provided with BSIRs to show progress made in meeting strategic goals and objectives. Future awards and fund drawdowns may be withheld if these reports are delinquent. The final BSIR is due 120 days after the end date of the award period.

Grant Reporting Timeline

Based on a one year period of performance, ODP expects most grants will have a reporting schedule similar to timeline below. Most grants will have three submissions over the course of the period of performance including two BSIR submissions and one final BSIR submission. The FY05 BZPP is exempt from the FY05 ISIP. **The first grant report submission for the BZPP in 2005 is the FY05 BSIR due on July 31, 2005.**



Grant Reporting Timeline

Required Submissions: BSIR (biannually).

D. Monitoring

Grant recipients will be monitored periodically by ODP Preparedness Officers and/or PSD Field Security Detachments and Protective Security Advisors (PSAs) to ensure that the program goals, objectives, timelines, budgets, equipment acquisition, and other related program criteria are being met. ODP will be responsible for the financial monitoring of the program and PSD will be responsible for the monitoring of the development of the BZPs, VRPPs, and all vulnerability site assessment related activities. Monitoring will be accomplished through a combination of office-based and on-site monitoring visits. Monitoring will involve the review and analysis of the financial, programmatic, operational, and administrative issues relative to each project/site, and will identify areas where technical assistance and other support may be needed.

The SAA is also responsible for monitoring subgrantee activities to provide reasonable assurance that the subgrantee administers federal awards in compliance with federal and state requirements. Responsibilities include the accounting of receipts and expenditures, cash management, the maintaining of adequate financial records, and the refunding of expenditures disallowed by audits.

E. Grant Close-out Process

Within 120 days after the end of the grant period, the grantee will submit a final FSR and a final BSIR detailing all accomplishments throughout the project. After both of these reports have been reviewed and approved by the ODP Preparedness Officer and PSD, a Grant Adjustment Notice (GAN) will be completed to close-out the grant. The GAN will indicate the project as being

closed, list any remaining funds that will be de-obligated, and address the requirement of maintaining the grant records for three years from the date of the final FSR. After the financial information is received and approved by the OJP Office of the Comptroller, the grant will be identified as "Closed by the Office of the Comptroller."

Required Submissions: 1) Final SF-269 FSR; 2) Final BSIR.

APPENDIX A

SAMPLE AWARD
PACKAGE

SAMPLE AWARD PACKAGE

TAB 1: SAMPLE REVIEW OF AWARD

Office of Justice Programs
Post Award Instructions for ODP Awards

Step 1. Review Award and Special Conditions Document.
Carefully read the award and any special conditions or other attachments. There is an original plus one copy of the award page.

If you agree with the terms and conditions, the authorized official should sign and date both the original and the copy of the award document page in Block 19. You should maintain a copy and return the original signed documents to:

Office of Justice Programs
Attn: Control Desk - ODP Award
810 Seventh Street, NW – 5th Floor
Washington, DC 20531

If you do not agree with the terms and conditions, contact the awarding ODP Preparedness Officer as noted in the award package.

Step 2. Read Guidelines.
Become familiar with the "OJP Financial Guide" which is available through the internet at the OJP, Office of the Comptroller website:
http://www.ojp.usdoj.gov/oc/. New award recipients are automatically placed on a mailing list to receive future Guides and their change sets.

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

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

TAB 2: SAMPLE POST AWARD INSTRUCTION

U. S. Department of Justice
Office of Justice Programs
Office of the Comptroller

Post Award Instructions

OJP is currently responsible for the financial administration of grants awarded by the ODP.

The following is provided as a guide for the administration of awards from ODP. Forms and other documents illustrating each step are attached.

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

If you do not agree with the terms and conditions as written, contact your ODP Preparedness Officer.

Step 2. Read Guidelines.
Read and become familiar with the "OJP Financial Guide" and related material (refer to Step 2 attachment).

Step 3. Complete and Return ACH Form.
The Automated Clearing House (ACH) Vendor/Miscellaneous Payment Enrollment Form (refer to Step 3 attachment) is used to arrange direct deposit of funds into your designated bank account.

Step 4. Access to Payment Systems.
OJP uses two payment systems: Phone Activated Paperless System (PAPRS) and Letter of Credit Electronic Certification System (LOCES) (refer to Step 4 attachment). Current LOCES users will see the addition of new ODP grants on the LOCES grant number listing as soon as the ODP award acceptance has been received. PAPRS grantees will receive a letter with the award package containing their PIN to access the system and Grant ID information.

Step 5. Reporting Requirements.
Reporting requirements must be met during the life of the grant (refer to the OJP Financial Guide for a full explanation of these requirements, special conditions and any applicable exceptions). The payment systems contain edits which will prevent access to funds if reporting requirements are not met on a timely basis. Refer to Step 5 attachments for forms, due date information, and instructions.

Step 6. Questions about your award?

A reference sheet is provided containing frequently asked financial questions and answers. If you have questions concerning this checklist or any financial aspect of your award, contact the Office of the Comptroller's Customer Service Center at 1-800-458-0786 or by email at askoc@ojp.usdoj.gov**.** Customer Service staff are available from 9:00 a.m. to 6:00 p.m. EST, Monday-Friday.

APPENDIX B

PUBLIC SAFETY COMMUNICATIONS AND INTEROPERABILITY GUIDANCE

PUBLIC SAFETY COMMUNICATIONS AND INTEROPERABILITY GUIDANCE

In May 2004, ODP adopted language about grant guidance developed by SAFECOM in an effort to ensure interoperability through the various layers of federal, state and local government. (See ODP Information Bulletin #113). SAFECOM developed this general grant criteria in concert with representatives of the public safety community in an effort to coordinate the way in which funding is allocated and to maximize the prospects for interoperable communications.

The intent of the SAFECOM grant guidance is to ensure that the communications equipment being procured will lead to improved multi-disciplinary and/or multi-jurisdictional interoperable public safety communications. The grant guidance provides a list of questions to be answered in order to demonstrate how the applicants proposed project would enhance interoperability. The guidance also encourages that, where appropriate, applicants purchase equipment that meets standards that have been developed and adopted by the public safety communications community–American National Standards Institute (ANSI)/TIA/EIAA-102 Phase 1 (Project 25) suite of standards. This recommendation is intended for government-owned or -leased land mobile public safety radio equipment, and its purpose is to make sure that such equipment or systems are capable of interoperating with other public safety land mobile equipment or systems. It is not intended to apply to commercial services that offer other types of interoperability solutions and does not exclude any application if it demonstrates that the system or equipment being proposed will lead to enhanced interoperability. The grant guidance does not propose to preclude funding of non-Project 25 equipment when there are compelling reasons for using other solutions. Absent these compelling reasons, ODP intends that Project 25 equipment will be preferred for digital systems to which the standard applies.

The SAFECOM interoperable communications guidance addresses the following issues:

- Criteria
    - Personnel Involved with Public Safety Communications Interoperability
    - Lifecycle of Public Safety Communications Projects
    - Common Public Safety Communications Goals
    - Common Criteria for All Grant Applicants
    - Standards
    - Governance

- Criteria for Public Safety Communications Equipment Grants

    - Building, Upgrading, Enhancing, Replacing and Maintaining Public Safety Communications Systems and Equipment

- Supplemental Criteria for Public Safety Equipment Grants
    - Planning for Public Safety Communication Systems
    - Training Public Safety Staff on Issues Related to Emergency Response Communications
    - Managing Public Safety Communications Projects
    - Generic Examples of Linking Disparate Public Safety Communications Systems

The SAFECOM grant guidance materials are available in their entirety on the SAFECOM website (http://www.safecomprogram.gov) in the electronic library. (See http://www.safecomprogram.gov/libresults.cfm?libid=431&secid=3.) They can also be accessed through ODP Information Bulletin #113, posted on the ODP website at http://www.ojp.usdoj.gov/odp/docs/bulletins.htm.

APPENDIX C

LIST OF TERMS

List of Terms

A		
	AAR	After Action Reports
	AEL	Authorized Equipment List
	ANSI	American National Standards Institute
	APCO	Association of Public-Safety Communications Officials
B		
	BSIR	Biannual Strategy Implementation Reports
	BZP	Buffer Zone Plan
	BZPP	Buffer Zone Protection Program
C		
	CAPR	Categorical Assistance Progress Reports
	CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
	CFDA	Catalog of Federal Domestic Assistance
	CI	Critical Infrastructure
	CIP	Critical Infrastructure Protection
	CSID	Centralized Scheduling and Information Desk
D		
	D&B	Dun and Bradstreet
	DHS	U.S. Department of Homeland Security
	DLA	Defense Logistics Agency
	DOJ	U.S. Department of Justice
	DPETAP	Domestic Preparedness Equipment Technical Assistance Program
	DUNS	Data Universal Numbering System
E		
	EA	Environmental Assessment
	EIS	Environmental Impact Statement
F		
	FAR	Federal Acquisition Regulations
	FOIA	Freedom of Information Act
	FSR	Financial Status Report
G		
	GAN	Grant Adjustment Notice
	GMS	Grants Management System
H		
	HSAS	Homeland Security Advisory System
	HSGP	Homeland Security Grant Program
	HSPTAP	Homeland Security Preparedness Technical Assistance Program
I		
	IAB	Interagency Board

	IAIP	DHS Information Analysis and Infrastructure Protection Directorate
	IP	Infrastructure Protection
	ISIP	Initial Strategy Implementation Plan
K		
	KA	Key Asset
	KR	Key Resource
L		
	LEP	Limited English Proficient
	LETPP	Law Enforcement Terrorism Prevention Program
	LLIS	Lessons Learned Information Sharing
	LOCES	Letter of Credit Electronic Certification System
M		
	M&A	Management and Administrative
	MIPT	Memorial Institute for the Prevention of Terrorism
N		
	NADB	National Asset Database
	NCJA	National Criminal Justice Association
	NEPA	National Environmental Policy Act
O		
	OC	Office of the Comptroller
	ODP	Office for Domestic Preparedness
	OJP	Office of Justice Programs
	OMB	Office of Management and Budget
P		
	PAPRS	Phone Activated Paperless Request System
	POC	Point of Contact
	PSA	Protective Security Advisor
	PSD	Protective Security Division
S		
	S&T	Science and Technology
	SAA	State Administrative Agency
	SEL	Standardized Equipment List
	SHSAS	State Homeland Security Assessments and Strategies
	SHSP	State Homeland Security Program
	SHSS	State Homeland Security Strategy
	SLGCP	DHS Office of State and Local Government Coordination and Preparedness
	SPOC	Single Point of Contact
T		
	TA	Technical Assistance
	TVA	Threat and Vulnerability Assessment

U

UAWG	Urban Area Working Group

V

VRPP	Vulnerability Reduction Purchase Plan

W

WMD	Weapons of Mass Destruction