



U.S. DEPARTMENT OF HOMELAND SECURITY

Fiscal Year 2008

FREIGHT RAIL SECURITY GRANT PROGRAM

PROGRAM GUIDANCE AND APPLICATION KIT

February 2008



U.S DEPARTMENT OF HOMELAND SECURITY

CONTENTS

| | |
|---|-----|
| CONTENTS | I |
| INTRODUCTION..... | 1 |
| PART I AVAILABLE FUNDING AND ELIGIBLE APPLICANTS | 5 |
| PART II APPLICATION EVALUATION PROCESS | 11 |
| PART III PROGRAM REQUIREMENTS..... | 13 |
| APPENDIX A. ALIGNMENT WITH THE NATIONAL PREPAREDNESS ARCHITECTURE..... | A-1 |
| APPENDIX B. FRSGP ALLOWABLE EXPENSES..... | B-1 |
| APPENDIX C. <i>GRANTS.GOV</i> QUICK-START INSTRUCTIONS | C-1 |
| APPENDIX D. INVESTMENT JUSTIFICATION..... | D-1 |
| APPENDIX E. VULNERABILITY ASSESSMENT..... | E-1 |
| APPENDIX F. SECURITY PLAN..... | F-1 |
| APPENDIX G. FRONTLINE EMPLOYEE SECURITY TRAINING..... | G-1 |
| APPENDIX H. SAMPLE BUDGET DETAIL WORKSHEET | H-1 |
| APPENDIX I. AWARD AND REPORTING REQUIREMENTS..... | I-1 |
| APPENDIX J. ADDITIONAL RESOURCES | J-1 |
| APPENDIX K. VULNERABILITY ASSESSMENT AND SECURITY PLAN CERTIFICATION FORM TO APPLY FOR RAILROAD FRONTLINE EMPLOYEE TRAINING..... | K-1 |
| APPENDIX L. VULNERABILITY ASSESSMENT AND SECURITY PLAN CERTIFICATION FORM FOR 49 CFR PART 172..... | L-1 |

INTRODUCTION

The Freight Rail Security Grant Program (FRSGP) is a new component of the Transit Security Grant Program (TSGP), which is one of five grant programs that constitute the Department of Homeland Security (DHS) Fiscal Year (FY) 2008 focus on infrastructure protection activities. The FRSGP is one tool among a comprehensive set of measures authorized by Congress and implemented by the Administration to help strengthen the Nation's critical infrastructure against risks associated with potential terrorist attacks.

The FRSGP was created as a result of Public Law (PL) 110-53, entitled "Implementing Recommendations of the 9/11 Commission Act of 2007." In FY 2008, the FRSGP will fund security training for railroad frontline employees,¹ the completion of vulnerability assessments, and the development of security plans within the Freight Rail industry.

The purpose of this package is to provide: (1) an overview of the FY 2008 FRSGP; and (2) the formal grant guidance and application materials needed to apply for funding under the program. Also included is an explanation of DHS management requirements for implementation of a successful application.

Making an application for significant Federal funds under programs such as this can be complex. The Department's job is to provide clear guidance and efficient application tools to assist applicants. DHS customers are entitled to effective assistance during the application process, and transparent, disciplined management controls to support grant awards. The Department intends to be good stewards of precious Federal resources and commonsense partners with State, local, and private sector colleagues.

The Department understands that individual railroad carriers have unique needs and tested experience on how best to reduce risk locally. DHS subject matter experts will evaluate grant applications with the overall goal of reducing risk, but will also be sensitive to local needs and approaches. In short, DHS commits to respect flexibility and local innovation as the Department funds national homeland security priorities.

A. Federal Investment Strategy

The FRSGP is an important part of the Administration's larger, coordinated effort to strengthen homeland security preparedness, including the security of America's critical infrastructure. The FRSGP implements objectives addressed in a series of post-9/11 laws, strategy documents, plans, Executive Orders, and Homeland Security Presidential Directives (HSPDs) outlined in Appendix A. Of particular significance are the National Infrastructure Protection Plan (NIPP), the transportation sector-specific plan, the freight rail modal annex, and Executive Order 13416 (Strengthening Surface Transportation Security). The National Preparedness Guidelines are an all-hazards vision regarding the Nation's four core preparedness objectives: prevent, protect against, respond to, and recover from terrorist attacks and catastrophic natural disasters.

¹ As defined in § 1501 of PL 110-53.

The National Preparedness Guidelines define a vision of what to accomplish and a set of tools to forge a unified national consensus about what to do and how to work together at the Federal, State, local, and Tribal levels. Private sector participation is integral to the Guidelines' success. It outlines 15 scenarios of terrorist attacks or national disasters that form the basis of much of the Federal exercise and training regime. In addition, 37 critical target capabilities are identified that DHS is making the focus of key investments with State, local and Tribal partners.

DHS expects its critical infrastructure partners—including recipients of FRSGP grants—to be familiar with this national preparedness architecture and to incorporate elements of this architecture into their planning, operations, and investment to the degree practicable. Our funding priorities outlined in this document reflect National Preparedness Guidelines priority investments as appropriate. Programmatic requirements or priority investment categories reflecting the national preparedness architecture for this grant program are identified below.

B. Funding Priorities

The funding priorities for the FY 2008 FRSGP reflect the Department's overall investment strategy as well as requirements of PL 110-53. The key goals of the FY 2008 FRSGP are to establish the basis for future capital security improvements by funding vulnerability assessments and security plans and to provide training to frontline personnel.

The Department, in alignment with PL 110-53, identifies the following specific priorities for the FY 2008 FRSGP as the only allowable uses of funds under this year's program:

- 1. Vulnerability Assessments and Security Plans.** Freight railroad vulnerability assessments will provide a broader picture of the mode's preparedness, as well as security risks that need to be mitigated. In an effort to "buy down" these security risks, security plans will help target resources and mitigation strategies toward gaps in the mode's security identified by the vulnerability assessments. The information captured in the vulnerability assessments and security plans (including any all mitigation strategies) will form the basis of funding priorities for this grant program in future years, as appropriate. Freight railroad carriers without complete vulnerability assessments and security plans will not be considered for other projects in future grant years. DHS recognizes that Class II and Class III railroad carriers vary greatly in their size and scope of operations. Therefore, eligible railroad carriers should request the funds they believe are necessary for comprehensive vulnerability assessments and security plans. Please note that all applicants will be required to certify the existence of both a vulnerability assessment and security plan that comply fully with the requirements of 49 CFR 172.802 to be eligible for any funding under the FY 2008 FRSGP. A certification form template can be found in Appendix L, and should be submitted as part of the application submission.

- 2. Security training for railroad frontline employees.** Effective employee training programs address individual employee responsibilities and provide heightened security awareness. Training should cover adequately assessing and reporting incidents, appropriate employee response, crew communication and coordination, and incident evacuation procedures. For example, a well trained railroad employee can help ensure that trespassers on railroad property are identified and reported. Please refer to Appendix G for further explanation of necessary components of security awareness and emergency response training.

Eligible applicants² are divided into two groups based on the types of projects they can apply for: Class I railroad carriers and Class II/III railroad carriers. Eligible Class I railroad carriers may ONLY request funding for security awareness and emergency response training for railroad frontline employees. This grant program does not cover the expenses associated with conducting a vulnerability assessment or developing a security plan for Class I carriers. In order to be eligible to request this training funding, Class I carriers must certify to DHS that they have completed both a vulnerability assessment and a security plan that meet the requirements detailed in Appendix E (Vulnerability Assessment) and Appendix F (Security Plan), respectively.

Eligible Class II and Class III railroad carriers may use grant funds received under this program to complete a vulnerability assessment and security plan that meet the requirements outlined in Appendices E and F. If a plan has already been completed but does not meet these requirements, the applicant may request funding to conduct a new vulnerability assessment and to develop a new security plan to meet the requirements. Upon completion of the vulnerability assessment and security plan, eligible Class II and Class III railroad carriers may request funding for security awareness and emergency response training for railroad frontline employees. In order for these training projects to be funded, the carrier must first certify, using Appendix K, that the requirements for vulnerability assessments and security plans as detailed in Appendix E and Appendix F have been met. If these items have already been completed, an eligible applicant may request funds for training. More information on training can be found in Appendix G.

In order to request FY 2008 FRSGP funds, applicants must complete and submit an Investment Justification, the outline of which is provided in Appendix D.

C. Allowable Expenses

Specific investments made in support of the funding priorities discussed above generally fall into three categories:

1. Vulnerability Assessments and Security Plans
2. Training
3. Management and Administration

² The term “eligible applicants” is defined in Part I., Section B of this document.

Awardees must commit to minimum training standards to be set by the Department for all Federally-funded security personnel. Costs associated with meeting these training standards will be an allowable expense.

Freight railroad carriers that submit training requests should request “basic” training before “follow-on” training courses. Requests for follow-on training courses should include a statement that the basic training course has been fulfilled or is not applicable. Requests for follow-on training should include the following information:

- Type, name, and vendor of the basic training classes frontline employees have received; and
- Dates when the employees received the training, including how many employees attended each class.

Appendix B provides additional detail about each of these allowable expense categories, and identifies several specific unallowable costs. Appendices E and F provide templates and the necessary elements of a vulnerability assessment and a security plan.

Please note that in accordance with Public Law 110-53 applicants must have developed a vulnerability assessment and a security plan prior to requesting and receiving funds for the training of frontline employees.³

³ PL 110-53 §1513(a)(5)

PART I

AVAILABLE FUNDING AND ELIGIBLE APPLICANTS

A. Available Funding

The FY 2008 FRSGP will provide **\$15 million** for eligible applicants to conduct vulnerability assessments, develop security plans, and for the security training of frontline employees.

B. Selection of Eligible Applicants

Eligible applicants for the FY 2008 FRSGP are determined by DHS as Class I, II, and III freight railroad carriers that transport Security-Sensitive Materials (SSM). A regulation defining SSM is currently under development; however, a definition of SSM is provided below specifically for the purposes of the FY 2008 FRSGP.

As designated by the Surface Transportation Board, a Class I railroad carrier is defined as a railroad with annual operating revenues for 2005 over \$319.2 million; a Class II railroad carrier is defined as a railroad with annual operating revenues between \$25.5 million and \$319.2 million; and a Class III railroad carrier is defined as a railroad with annual operating revenues of less than \$25.5 million.

Applicants must also meet the following criteria in order to be eligible:

- Transport Rail SSM. For the purpose of this grant, SSM is defined as: 1) more than 2,268 kg (5,000 lbs.) in a single carload of a Division 1.1, 1.2, or 1.3 explosive; 2) a tank car containing a material poisonous by inhalation, as defined in 49 CFR 171.8, including anhydrous ammonia but excluding residue quantities of these materials; and 3) a highway route-controlled quantity of a Class 7 (radioactive) material, as defined in 49 CFR 173.403.
- Operate in or through at least one high population-density area, as subject to the forthcoming “Rail Transportation Security Final Rule,” and as identified in Table 1 below.
- Certify they have developed and adhere to a vulnerability assessment and security plan that conforms to the requirements of 49 CFR 172.802.⁴

Class I freight railroad carriers may apply for training funds if they **certify they have completed a vulnerability assessment and security plan that meet the requirements outlined in Appendices E and F**. This grant program does not cover

⁴ The Secretary has determined that the security plans and the vulnerability assessment required under this section is sufficient for initial eligibility and the requirements of section 1513 Railroad Security Assistance of PL 110-53 “Implementing Recommendations of the 9/11 Commission Act of 2007.”

the expenses associated with conducting a vulnerability assessment or developing a security plan for Class I carriers.

Eligible Class II and Class III railroad carriers that have completed a vulnerability assessment and security plan that comply with 49 CFR 172.802 may request funding to conduct a new vulnerability assessment and to develop a new security plan security plan to meet the requirements detailed in Appendix E and Appendix F. Funds may also be used to improve upon an existing security plan to meet the requirements of Appendix F. Eligible Class II and Class III railroad carriers may request funding for security awareness and emergency response training for railroad frontline employees if they can certify, using Appendix K, that the requirements for vulnerability assessments and security plans as detailed in Appendix E and Appendix F have been met by their existing vulnerability assessment and implemented security plan.

Please refer to Appendices K and L for a certification templates. These certifications should be submitted as part of the grant application, as applicable.

Table 1. High Population-Density Areas

| State | Population Area | Geographic Area | Definitions |
|-------|------------------------|---|---|
| AZ | Phoenix Area | Chandler, Gilbert, Glendale, Mesa, Peoria, Phoenix, Scottsdale, Tempe | City of Phoenix; Maricopa County, and the three tribal nations of Salt River Pima, Fort McDowell, and Gila River |
| CA | Anaheim/Santa Ana Area | Anaheim, Costa Mesa, Garden Grove, Fullerton, Huntington Beach, Irvine, Orange, Santa Ana | Cities of Anaheim and Santa Ana; Orange County; unincorporated areas of Orange County; Cities of Brea, Buena Park, Cypress, Fullerton, Garden Grove, La Habra, La Palma, Los Alamitos, Orange, Placentia, Seal Beach, Stanton, Westminster, Villa Park, Yorba Linda, Irvine, Costa Mesa, Fountain Valley, Huntington Beach, Laguna Niguel, Newport Beach, Tustin, San Juan Capistrano, Laguna Beach, Aliso Viejo, Dana Point, Laguna Hills, Laguna Woods, Lake Forest, Mission Viejo, Rancho Santa Margarita, San Clemente, and University of California at Irvine Police Department. |
| | Bay Area | Berkeley, Daly City, Fremont, Hayward, Oakland, Palo Alto, Richmond, San Francisco, San Jose, Santa Clara, Sunnyvale, Vallejo | Cities of San Francisco, San Jose and Oakland and Counties of San Francisco, Santa Clara, Alameda ; Counties of Marin, San Mateo, Monterey, San Benito, Santa Cruz; and the Golden Gate Bridge District; Cities of Campbell, Cupertino, Gilroy, Los Altos, Los Altos Hills, Milpitas, Monte Sereno, Morgan Hill, Mountain View, Palo Alto, Santa Clara, Saratoga, Sunnyvale, the town of Los Gatos, the Port/Airport (Oakland), Berkeley, San Leandro, Alameda, Emeryville, and Piedmont; Secondary Area: entire Counties of Alameda and Contra Costa. |

U.S. DEPARTMENT OF HOMELAND SECURITY – TSGP FREIGHT RAIL SECURITY GRANT PROGRAM

| State | Population Area | Geographic Area | Definitions |
|-------|-----------------------------|--|--|
| | Los Angeles/Long Beach Area | Burbank, Glendale, Inglewood, Long Beach, Los Angeles, Pasadena, Santa Monica, Santa Clarita, Torrance, Simi Valley, Thousand Oaks | Cities of Long Beach and Los Angeles and County of Los Angeles; Los Angeles County Unincorporated; Cities of Beverly Hills, Burbank, Carson, Commerce, Culver City, El Segundo, Glendale, Hawthorne, Inglewood, Pasadena, San Fernando, Santa Monica, Torrance, Vernon, West Hollywood, Bellflower, Carson, Compton, Hawaiian Gardens, Lakewood, Paramount, and Signal Hill. |
| | Sacramento Area | Elk Grove, Sacramento | City and County of Sacramento; Cities of Citrus Heights, Elk Grove, Folsom, Rancho Cordova, Rocklin, Roseville, and West Sacramento; the eastern portion of Yolo County adjacent to the City of West Sacramento, and the southern portion of Placer County adjacent to the cities of Roseville and Rocklin. |
| | San Diego Area | Chula Vista, Escondido, and San Diego | City and County of San Diego, inclusive of cities of Carlsbad, Chula Vista, Coronado, Del Mar, El Cajon, Encinitas, Escondido, Imperial Beach, La Mesa, Lemon Grove, National City, Oceanside, Poway, San Marcos, Santee, Solana Beach and Vista. |
| CO | Denver Area | Arvada, Aurora, Denver, Lakewood, Westminster, Thornton | City and County of Denver; Counties of Adams, Jefferson and Arapahoe; the entities of City of Arvada, Arvada Fire District, City of Aurora, Commerce City, City of Englewood, City of Glendale, City of Lakewood, City of Littleton, Littleton Fire District, City of Sheridan, Cherry Hills Village, Cunningham Fire District, Jefferson County Greenwood Village, Greater Brighton Fire District, North Washington Fire District, South Adams County Fire District, South Metro Fire Rescue, Southwest Adams Fire District, West Metro Fire Rescue, and City of Wheat Ridge. |
| DC | National Capital Region | National Capital Region | District of Columbia; Counties of Montgomery and Prince George's (MD); Counties of Arlington, Fairfax, Prince William, and Loudon (VA); Cities of Falls Church, Manassas, Manassas Park, Fairfax, and Alexandria (VA). |
| FL | Fort Lauderdale Area | Fort Lauderdale, Hollywood, Miami Gardens, Miramar, Pembroke Pines | Fort Lauderdale, Hollywood, Miami Gardens, Miramar, Pembroke Pines |
| | Jacksonville Area | Jacksonville | City of Jacksonville; Duval County; Counties of Nassau, Baker, Union, Bradford, Alachua, Clay, Putnam, St. Johns, Flagler, Marion, Levy, and Gilchrist. |
| | Miami Area | Hialeah, Miami | City of Miami; Counties of Miami-Dade, Broward, and Monroe. |

U.S. DEPARTMENT OF HOMELAND SECURITY – TSGP FREIGHT RAIL SECURITY GRANT PROGRAM

| State | Population Area | Geographic Area | Definitions |
|-------|-------------------|-----------------------------------|---|
| | Orlando Area | Orlando | City of Orlando; Orange County; Counties of Seminole, Brevard, Osceola, and Lake. |
| | Tampa Area | Clearwater, St. Petersburg, Tampa | City of Tampa; Hillsborough County; Pinellas County, inclusive of Clearwater, Temple Terrace, and St. Petersburg. |
| GA | Atlanta Area | Atlanta | City of Atlanta; Counties of Fulton and DeKalb Georgia; Supported by the contiguous counties of Gwinnett, Rockdale, Henry, Clayton, Fayette, Cobb, and Douglas. |
| HI | Honolulu Area | Honolulu | City of Honolulu; Honolulu County (Island of Oahu). |
| IL | Chicago Area | Chicago | City of Chicago; Cook County, inclusive of 128 municipalities. |
| IN | Indianapolis Area | Indianapolis | City of Indianapolis; Counties of Hamilton and Marion. |
| KY | Louisville Area | Louisville | City of Louisville; Louisville/Jefferson County Metro Government; inclusive of the cities of Jeffersontown, St. Matthews, Shively, and Anchorage. Secondary area inclusive of the Kentucky counties of Bullitt, Henry, Meade, Nelson, Oldham, Shelby, Spencer, and Trimble. |
| LA | Baton Rouge Area | Baton Rouge | City of Baton Rouge; East Baton Rouge Parish; Louisiana Homeland Security Region 2 which includes East and West Baton Rouge Parish, East and West Feliciana Parish, Ascension Parish, LA Livingston Parish, Iberville Parish, and Pointe Coupee Parish. |
| | New Orleans Area | New Orleans | City of New Orleans; Orleans Parish; Parishes of Jefferson, St. Bernard, and Plaquemines. |
| MA | Boston Area | Boston, Cambridge | City of Boston; Communities of Brookline, Cambridge, Chelsea, Everett, Quincy, Revere, Winthrop, and Somerville. |
| MD | Baltimore Area | Baltimore | City of Baltimore; Counties of Baltimore and Anne Arundel; City of Annapolis; Counties of Carroll, Harford, and Howard. |
| MI | Detroit Area | Detroit, Sterling Heights, Warren | City of Detroit; Wayne County; Counties of Macomb, Oakland, Washtenaw, Monroe, and St. Clair. |
| MN | Twin Cities Area | Minneapolis, St. Paul | Cities of Minneapolis and St. Paul; Counties of Hennepin, Ramsey, and Dakota County. |

U.S. DEPARTMENT OF HOMELAND SECURITY – TSGP FREIGHT RAIL SECURITY GRANT PROGRAM

| State | Population Area | Geographic Area | Definitions |
|--------------|-------------------------|---|--|
| MO | Kansas City Area | Independence, Kansas City (MO), Kansas City (KS), Olathe, Overland Park | Cities of Kansas City (MO) and Kansas City (KS); Counties of Cass, Clay, Jackson, Platte, and Ray (MO); Counties of Johnson, Leavenworth, and Wyandotte (KS). |
| | St. Louis Area | St. Louis | City and County of St. Louis; Counties of St. Charles, Franklin, and Jefferson (MO); Counties of St. Clair, Madison, and Monroe (IL). |
| NC | Charlotte Area | Charlotte | City of Charlotte; Mecklenburg County; Counties of Union, Cabarrus, Stanly, Iredell, Catawba, Lincoln, Gaston; supported by York and Lancaster in South Carolina. |
| NE | Omaha Area | Omaha | City of Omaha; Counties of Douglas, Sarpy, and Washington. |
| NJ | Jersey City/Newark Area | Elizabeth, Jersey City, Newark | Cities of Jersey City and Newark; Counties of Essex, Bergen, Hudson, Morris, Passaic, and Union. |
| NV | Las Vegas Area | Las Vegas, North Las Vegas | City of Las Vegas; Clark County. |
| NY | Buffalo Area | Buffalo | City of Buffalo; Counties of Erie and Niagara. |
| | New York City Area | New York City, Yonkers | City of New York; Counties of Nassau, Suffolk, and Westchester; Port Authority of New York and New Jersey. |
| OH | Cincinnati Area | Cincinnati | City of Cincinnati; Hamilton County, and the 48 local jurisdictions within the county; Counties of Adams, Brown, Butler, Clermont, Clinton, Highland, Warren (OH); Counties of Boone, Campbell, Kenton (KY), and County of Dearborn (IN). |
| | Cleveland Area | Cleveland | City of Cleveland; Cuyahoga County, inclusive of nine Cuyahoga Community Regions - Chagrin, Cleveland, Cuyahoga, Heights, Hillcrest, Southcentral, Southeast, Southwest, and Westshore, and the local jurisdictions therein. |
| | Columbus Area | Columbus | City of Columbus; Franklin County; the cities of Bexley, Columbus, Dublin, Grandview Heights, Grove City, Hilliard, Reynoldsburg, Upper Arlington, Westerville, Worthington; Villages of Brice, Canal Winchester, Groveport, Harrisburg, Lockbourne, Marble Cliff, Minerva Park, New Albany, Obetz, Urbancrest, Valleyview; Townships of Blendon, Brown, Clinton, Franklin, Hamilton, Jackson, Jefferson, Madison, Mifflin, Norwich, Perry, Plain, Pleasant, Prairie, Sharon, Truro, Washington. |

U.S. DEPARTMENT OF HOMELAND SECURITY – TSGP FREIGHT RAIL SECURITY GRANT PROGRAM

| State | Population Area | Geographic Area | Definitions |
|-------|----------------------------------|--|---|
| | Toledo Area | Oregon, Toledo | City of Toledo; Lucas County; Cities of Maumee, Oregon, Sylvania, and Toledo; Villages of Berkey, Harbor View, Holland, Ottawa Hills, Waterville, Whitehouse, and a portion of the Village of Swanton (the other portion being in the County of Fulton); Townships of Jerusalem, Harding, Monclova, Providence, Richfield, Spencer, Springfield, Sylvania, Swanton, Washington, and Waterville. |
| OK | Oklahoma City Area | Norman, Oklahoma City | City of Oklahoma; Counties of Oklahoma, Canadian, and Cleveland; including the boundaries of OKOHS Regions 6 and 8 (Counties of McClain, Lincoln, Pottawatomie, and Logan). |
| OR | Portland Area | Portland, Vancouver | City of Portland; Counties of Washington, Multnomah, Clackamas, and Columbia (OR); Clark County (WA). |
| PA | Philadelphia Area | Philadelphia | City of Philadelphia; Philadelphia County; Counties of Bucks, Chester, Delaware, and Montgomery. |
| | Pittsburgh Area | Pittsburgh | City of Pittsburgh; Counties of Allegheny, Armstrong, Beaver, Butler, Cambria, Fayette, Greene, Indiana, Lawrence, Mercer, Somerset, Washington, and Westmoreland. |
| TN | Memphis Area | Memphis | City of Memphis; Counties of Shelby, Fayette, Tipton, and Lauderdale (TN); Crittenden County (AR); Desoto County (MS). |
| TX | Dallas/Fort Worth/Arlington Area | Arlington, Carrollton, Dallas, Fort Worth, Garland, Grand Prairie, Irving, Mesquite, Plano | Cities of Dallas, Fort Worth, and Arlington; Counties of Dallas, Collin, Denton, Kaufman, Tarrant, Wise, Parker, Johnson, and Rockwall; DFW Airport, North Central Texas Council of Governments and DFW Hospital Council. |
| | Houston Area | Houston, Pasadena | City of Houston; Counties of Harris, Fort Bend, Montgomery, Brazoria, and Galveston; inclusive of the Transit Authority and the Port Authority. |
| | San Antonio Area | San Antonio | City of San Antonio; Counties of Bexar and Comal; and Alamo Area Councils of Government. |
| WA | Seattle Area | Seattle, Bellevue | City of Seattle; King County; Counties of Pierce and Snohomish. |
| WI | Milwaukee Area | Milwaukee | City of Milwaukee; Counties of Milwaukee, Waukesha, Washington County. |

PART II

APPLICATION EVALUATION PROCESS

This section summarizes the roles and responsibilities within DHS for managing the FY 2008 FRSGP, the overall timetable for the FY 2008 program, and core process and priorities that will be used to assess applications under the FY 2008 FRSGP. The next section provides detailed information about specific application requirements and the process for submission of applications.

A. FRSGP Program Management: Roles and Responsibilities at DHS

Within DHS, the Transportation Security Administration (TSA) by law has the lead for managing the Department's security oversight and security programs for the freight railroad industry. TSA provides railroad system subject matter expertise within DHS and determines the primary security architecture for the FRSGP. Its subject matter experts have the lead in crafting all selection criteria associated with the application review process. TSA coordinates daily with the DHS Chief Intelligence Officer to review intelligence reporting and develop intelligence risk assessments related to the transportation sector.

The Federal Emergency Management Agency (FEMA) has the lead for designing and operating the administrative mechanisms needed to manage the Department's core grant programs, including this grant program. In short, FEMA is responsible for ensuring compliance with all relevant Federal grant management requirements and delivering the appropriate grant management tools, financial controls, audits and program management discipline needed to support the FRSGP.

B. Overview – Application Deadline and Review Process

Completed applications must be submitted to DHS via www.grants.gov (see below for details about this Federal grants application tool) *no later than 11:59 PM EDT, March 17, 2008. DHS will evaluate and act on applications within 60 days following close of the application period.*

Applicants must comply with all administrative requirements—including Investment Justifications and application process requirements—described herein. Having met all administrative requirements, applications will be evaluated and ranked based on the evaluation criteria outlined below.

C. Evaluation Criteria

Separate factors will be considered in the evaluation of the Investment Justifications and Detailed Budgets depending on the type of project being requested, including

railroad frontline employee training or the development of a vulnerability assessment and security plan; however, all projects must be based in part on the railroad carrier's existing vulnerability assessment and security plan required under 49 CFR 172.802.

Training Evaluation Criteria:

1. **Compliance.** Projects will be evaluated by completeness of Investment Justifications and certification documents.
2. **Feasibility.** Projects will be evaluated on the feasibility of the plan for completing the training requested within the period of performance.

Security Plans and Vulnerability Assessment Evaluation Criteria:

1. **Compliance.** Projects will be evaluated by completeness of Investment Justifications and certification documents.
2. **Cost Appropriateness.** Projects will be evaluated and prioritized based on the cost appropriateness of the request to conduct the assessment and develop the plan, which will be determined by the carrier's characteristics such as assets, location, infrastructure, and size.
3. **Timelines.** Projects will be evaluated and prioritized on the ability of the applicant to complete the proposed project within the proposed timeframes.

DHS is committed to focusing the bulk of available funds on high-risk areas. As such, the risk associated with operating within each high-density population area will also be considered in the funding of project submissions. Risk is a function of average dwell time, track mileage, the volume of SSM being transported through the area, and other factors DHS considers relevant.

D. Grant Application Support from DHS

During the application and award periods, DHS will identify multiple opportunities, as allowed in the competitive process, for a cooperative dialogue between the Department and eligible freight railroad carriers. This commitment is intended to ensure a common understanding of the funding priorities and administrative requirements associated with the FY 2008 FRSGP and to help in submission of projects that will have the highest impact on reducing risks for eligible applicants.

PART III

PROGRAM REQUIREMENTS

This section provides detailed information about specific application requirements and the process for submission of applications.

A. General Program Requirements.

In administering the program, the eligible applicants must comply with the following general requirements of the FY 2008 FRSGP.

- 1. Management and Administration.** Any management and administrative (M&A) costs associated with individual projects submitted for consideration under the FY 2008 FRSGP must be included in the budget for that project. M&A costs may not exceed three percent (3%) of the funds awarded for each individual project.
- 2. Cost Share requirement.** The maximum Federal share of any project supported through FRSGP is 75% for public sector grantees and 50% for private sector grantees. Therefore, public sector grantees are required to provide non-Federal funding (cash or in-kind) of at least 25% of approved project costs for the FY 2008 FRSGP and private sector grantees are required to provide non Federal funding (cash or in-kind) of at least 50% of approved project costs. For example, for public sector grantees, if the total project cost is \$100,000, the maximum the DHS grant award is \$75,000 with the grantee required to provide the remaining 25%, or \$25,000, of the project cost. For private sector grantees, if the total project cost is \$100,000, the maximum DHS grant award is \$50,000.

B. Application Requirements.

The following steps must be completed using the on-line grants.gov system to ensure a successful application submission, however applicants should review the relevant program-specific sections of this Guidance for additional requirements that may apply.

- 1. Application via grants.gov.** DHS participates in the Administration's e-government initiative. As part of that initiative, all applicants must file their applications using the Administration's common electronic "storefront" -- grants.gov. Eligible applicants must apply for funding through this portal, accessible on the Internet at <http://www.grants.gov>.
- 2. Application deadline.** Completed Applications must be submitted to grants.gov no later than **11:59 PM EDT, March 17, 2008**.
- 3. Valid Central Contractor Registry (CCR) Registration.** The application process also involves an updated and current registration by the applicant. Eligible applicants must confirm CCR registration at <http://www.ccr.gov>, as well as apply for funding through grants.gov.

While registration with grants.gov and the CCR is a one-time process, new applicants are strongly encouraged to complete their registrations **at least ten (10) days prior** to the **March 17, 2008** application deadline.

4. **On-line application.** The on-line application must be completed and submitted using grants.gov after CCR registration is confirmed. The on-line application includes the following required forms and submissions:
 - Standard Form 424, Application for Federal Assistance
 - Standard Form 424B Assurances
 - Standard Form LLL, Disclosure of Lobbying Activities
 - Standard Form 424A, Budget Information
 - Certification Regarding Debarment, Suspension, and Other Responsibility Matters
 - Any additional Required Attachments

The program title listed in the Catalog of Federal Domestic Assistance (CFDA) is “*Rail and Transit Security Grant Program.*” The CFDA number is 97.075. When completing the online application, applicants should identify their submissions as new, nonconstruction applications.

5. **Project period.** The project period will be for a period not to exceed 36 months. Extensions to the period of performance will be considered on a case-by-case basis only through formal written requests to DHS.
6. **DUNS number.** The applicant must provide a Dun and Bradstreet Data Universal Numbering System (DUNS) number with their application. This number is a required field within grants.gov and for CCR Registration. Organizations should verify that they have a DUNS number, or take the steps necessary to obtain one, as soon as possible. Applicants can receive a DUNS number at no cost by calling the dedicated toll-free DUNS Number request line at 1-800-333-0505.
7. **Investment Justifications.** As part of the application process, applicants must develop a formal Investment Justification that addresses each initiative being proposed for funding. These Investment Justifications must demonstrate how each proposed project assists in the creation of security plans, facilitates the completion of a vulnerability assessment, or improves railroad frontline employee training. After submission, the Investment Justification will be reviewed to determine whether proposed investments address the funding priorities of this grant program.

Please see Appendix B as well for further guidance in preparing the Investment Justification.

8. Standard financial requirements.

8.1 -- Non-supplanting certification. This certification affirms that grant funds will be used to supplement existing funds, and will not replace (supplant) funds that have been appropriated for the same purpose. Applicants or grantees may be required to supply documentation certifying that a reduction in non-Federal resources occurred for reasons other than the receipt or expected receipt of Federal funds.

8.2 -- Assurances. Assurances forms (SF-424B and SF-424D) can be accessed at http://www07.grants.gov/agencies/approved_standard_forms.jsp. It is the responsibility of the recipient of the Federal funds to understand fully and comply with these requirements. Failure to comply may result in the withholding of funds, termination of the award or other sanctions. The applicant will be agreeing to these assurances upon the submission of the application.

8.3 -- Certifications regarding lobbying, debarment, suspension, other responsibility matters and the drug-free workplace requirement. This certification, which is a required component of the on-line application, commits the applicant to compliance with the certification requirements under 44 CFR Part 17, which contains provisions for *Government-wide Debarment and Suspension (Non-procurement) and Government-wide Requirements for Drug-Free Workplace (Grants)*; and 44 CFR part 18, *the New Restrictions on Lobbying*. All of these can be referenced at: http://www.access.gpo.gov/nara/cfr/waisidx_07/44cfrv1_07.html
http://www.access.gpo.gov/nara/cfr/waisidx_00/44cfrv1_00.html.

9. Technology requirements.

9.1 -- National Information Exchange Model (NIEM). DHS requires all grantees to use the latest NIEM specifications and guidelines regarding the use of Extensible Markup Language (XML) for all FRSGP awards. Further information about the required use of NIEM specifications and guidelines is available at <http://www.niem.gov>.

9.2 -- 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). DHS encourages grantees to align any geospatial activities with the guidance available on the FEMA website at <http://www.fema.gov/grants>.

9.3 -- 28 CFR Part 23 guidance. DHS requires that any information technology system funded or supported by FRSGP funds comply with 28 CFR Part 23, Criminal Intelligence Systems Operating Policies, if this regulation is determined to be applicable.

10. Administrative requirements.

10.1 -- Freedom of Information Act (FOIA). DHS recognizes that much of the information submitted in the course of applying for funding under this program or

provided in the course of its grant management activities may be considered law enforcement sensitive or otherwise important to national security interests. While this information under Federal control is subject to requests made pursuant to the Freedom of Information Act (FOIA), 5. U.S.C. §552, all determinations concerning the release of information of this nature are made on a case-by-case basis by the DHS FOIA Office, and may likely fall within one or more of the available exemptions under the Act. The applicant is encouraged to consult its own State and local laws and regulations regarding the release of information, which should be considered when reporting sensitive matters in the grant application, needs assessment and strategic planning process. The applicant may also consult FEMA regarding concerns or questions about the release of information under State and local laws. The grantee should be familiar with the regulations governing Sensitive Security Information (49 CFR Part 1520), as it may provide additional protection to certain classes of homeland security information.

10.2 -- Protected Critical Infrastructure Information (PCII). The PCII Program, established pursuant to the Critical Infrastructure Information Act of 2002 (CII Act), created a new framework, which enables State and local jurisdictions and members of the private sector voluntarily to submit sensitive information regarding critical infrastructure to DHS. The Act also provides statutory protection for voluntarily shared CII from public disclosure and civil litigation. If validated as PCII, these documents can only be shared with authorized users who agree to safeguard the information.

PCII accreditation is formal recognition that the covered government entity has the capacity and capability to receive and store PCII. DHS encourages all grantees to pursue PCII accreditation. Accreditation activities include signing an MOA with DHS, appointing a PCII Officer, and implementing a self-inspection program. For additional information about PCII or the accreditation process, please contact the DHS PCII Program Office at pcii-info@dhs.gov.

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

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

- *Title IX of the Education Amendments of 1972, as amended, 20 U.S.C. 1681 et. seq.* – discrimination on the basis of sex is eliminated in any education program or activity receiving Federal financial assistance.
- *The Age Discrimination Act of 1975, as amended, 20 U.S.C. 6101 et. seq.* – no person in the United States shall be, on the basis of age, excluded from participation in, denied the benefits of or subjected to discrimination under any program or activity receiving Federal financial assistance.

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

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

10.5 -- Integrating individuals with disabilities into emergency planning. Section 504 of the Rehabilitation Act of 1973, as amended, prohibits discrimination against people with disabilities in all aspects of emergency mitigation, planning, response, and recovery by entities receiving financial from DHS. In addition, Executive Order #13347, entitled "Individuals with Disabilities in Emergency Preparedness" signed in July 2004, requires the Federal Government to support safety and security for individuals with disabilities in situations involving disasters, including earthquakes, tornadoes, fires, floods, hurricanes, and acts of terrorism. Executive Order 13347 requires the federal government to, among other things, encourage consideration of the needs of individuals with disabilities served by State, local, and tribal governments in emergency preparedness planning.

DHS has several resources available to assist emergency managers in planning and response efforts related to people with disabilities and to ensure compliance with Federal civil rights laws:

- **Guidelines for Accommodating Individuals with Disabilities in Disaster:** The Guidelines synthesize the array of existing accessibility requirements into a user friendly tool for use by response and recovery

personnel in the field. The Guidelines are available at <http://www.fema.gov/oer/reference/>.

- **Disability and Emergency Preparedness Resource Center:** A web-based “Resource Center” that includes dozens of technical assistance materials to assist emergency managers in planning and response efforts related to people with disabilities. The “Resource Center” is available at <http://www.disabilitypreparedness.gov>.
- *Lessons Learned Information Sharing (LLIS)* resource page on **Emergency Planning for Persons with Disabilities and Special Needs:** A true one-stop resource shop for planners at all levels of government, non-governmental organizations, and private sector entities, the resource page provides more than 250 documents, including lessons learned, plans, procedures, policies, and guidance, on how to include citizens with disabilities and other special needs in all phases of the emergency management cycle.

LLIS.gov is available to emergency response providers and homeland security officials from the local, state, and federal levels. To access the resource page, log onto <http://www.LLIS.gov> and click on *Emergency Planning for Persons with Disabilities and Special Needs* under *Featured Topics*. If you meet the eligibility requirements for accessing Lessons Learned Information Sharing, you can request membership by registering online.

10.6 -- Compliance with the National Energy Conservation Policy and Energy Policy Acts. In accordance with the Consolidated Appropriations Act of 2008 (P.L. 110-161), all FY 2008 grant funds must comply with the following two requirements:

- None of the funds made available through shall be used in contravention of the Federal buildings performance and reporting requirements of Executive Order No. 13123, part 3 of title V of the National Energy Conservation Policy Act (42 USC 8251 et. Seq.), or subtitle A of title I of the Energy Policy Act of 2005 (including the amendments made thereby).
- None of the funds made available shall be used in contravention of section 303 of the Energy Policy Act of 1992 (42 USC13212).

10.7 -- Environmental and Historic Preservation Compliance. FEMA is required to consider the potential impacts to the human and natural environment of projects proposed for FEMA funding. FEMA, through its Environmental and Historic Preservation (EHP) Program, engages in a review process to ensure that FEMA-funded activities comply with various Federal laws including: National Environmental Policy Act, National Historic Preservation Act, Endangered Species Act, and Executive Orders on Floodplains (11988), Wetlands (11990) and Environmental Justice (12898). The goal of these compliance requirements is to protect our nation’s water, air, coastal, wildlife, agricultural, historical, and cultural resources, as well as to minimize potential adverse effects to children and low-income and minority

populations.

The grantee shall provide any information requested by FEMA to ensure compliance with applicable Federal EHP requirements. Any project with the potential to impact EHP resources (see Section E.8) cannot be initiated until FEMA has completed its review. Grantees may be required to provide detailed information about the project, including the following: location (street address or map coordinates); description of the project including any associated ground disturbance work, extent of modification of existing structures, construction equipment to be used, staging areas, access roads, etc; year the existing facility was built; natural, biological, and/or cultural resources present in the project vicinity; visual documentation such as site and facility photographs, project plans, maps, etc; and possible project alternatives.

For certain types of projects, FEMA must consult with other Federal and state agencies such as the U.S. Fish and Wildlife Service, State Historic Preservation Offices, and the U.S. Army Corps of Engineers, as well as other agencies and organizations responsible for protecting natural and cultural resources. For projects with the potential to have significant adverse effects on the environment and/or historic properties, FEMA's EHP review and consultation may result in a substantive agreement between the involved parties outlining how the grantee will avoid the effects, minimize the effects, or, if necessary, compensate for the effects.

Because of the potential for significant adverse effects to EHP resources or public controversy, some projects may require an additional assessment or report, such as an Environmental Assessment, Biological Assessment, archaeological survey, cultural resources report, wetlands delineation, or other document, as well as a public comment period. Grantees are responsible for the preparation of such documents, as well as for the implementation of any treatment or mitigation measures identified during the EHP review that are necessary to address potential adverse impacts. Grantees may use funds toward the costs of preparing such documents and/or implementing treatment or mitigation measures. Failure of the grantee to meet Federal, State, and local EHP requirements, obtain applicable permits, and comply with any conditions that may be placed on the project as the result of FEMA's EHP review may jeopardize Federal funding.

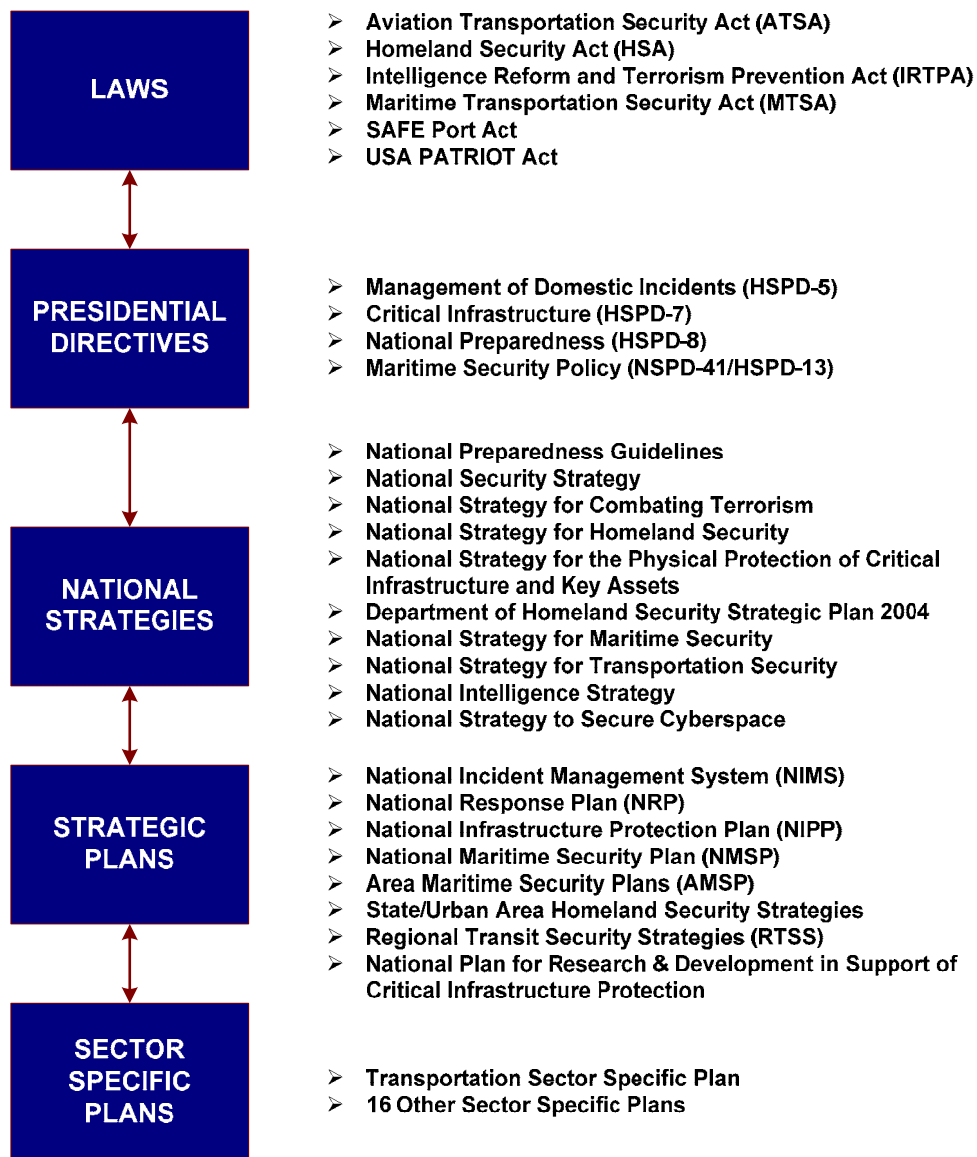
For more information on FEMA's EHP requirements, grantees should refer to FEMA's Information Bulletin #271, *Environmental Planning and Historic Preservation Requirements for Grants*.

Appendix A

Alignment with the National Preparedness Architecture

Figure 1, below, graphically summarizes key elements of the national preparedness architecture.

Figure 1
Laws, Strategy Documents, Directives and Plans that Impact the Grant Programs



Appendix B

FRSGP Allowable Expenses

A. Overview

Specific investments made in support of the funding priorities discussed above generally fall into one of the following three categories:

1. Vulnerability Assessments and Security Plans
2. Training
3. Management and Administration

The following provides guidance on allowable costs within each of these areas:

1. Development of Vulnerability Assessments and Security Plans. FY 2008 FRSGP funds may be used by Class II and Class III railroad carriers for the following types of activities:

Vulnerability Assessments

- Development of all required content, as specified in Appendix E, are allowable expenses.

Security Plans

- Development of all required content, as specified in Appendix F, are allowable expenses.

2. Training Costs. FY 2008 FRSGP funds may be used by Class I, II, and III railroad carriers—once they have completed and certified that they maintain and implement a vulnerability assessment and security plan that comports with Appendices E and F respectively—for the following training activities:

- **Training workshops and conferences.** Grant funds may be used to plan and conduct training workshops or conferences to include costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, travel and training plan development.
- **Certain full or part-time staff and contractors or consultants.** Full or part-time staff may be hired to support training-related activities. The applicant's formal written procurement policy or the Federal Acquisition Regulations must be followed.
- **Public sector employee overtime and backfill costs.** Payment of overtime expenses will be for work performed by award or sub-award employees in excess of the established work week (usually 40 hours). Further, overtime payments and backfill costs associated with sending personnel to training are allowable, provided that it is DHS approved training. Fringe benefits on overtime

hours are limited to Federal Insurance Contributions Act, Workers' Compensation and Unemployment Compensation. Overtime and backfill of private sector employees are not eligible.

- **Travel.** Travel costs (e.g., airfare, mileage, per diem, hotel) are allowable as expenses by public sector employees who are on travel status for official business related to the planning and conduct of the training project(s) or for attending DHS-approved courses or DHS-sponsored technical assistance programs. These costs must be in accordance with State law as highlighted in the 44 CFR.
Private sector employee travel costs are not allowable.
- **Supplies.** Supplies are items that are expended or consumed during the course of the planning and conduct of the training project(s) (e.g., copying paper, gloves, tape, and non-sterile masks).
- **Other items.** These costs may include the rental of space/locations for planning and conducting training, badges, and similar materials.

3. Management and Administration (M&A) costs. FY 2008 FRSGP funds may be used for the following M&A costs and is limited to three percent (3%) of the total grant award:

- Hiring of full-time or part-time staff or contractors/consultants to assist with the management of the FY 2008 FRSGP or the design, requirements, and implementation of the FRSGP.
- Hiring of full-time or part-time staff, contractors or consultants and M&A expenses related to pre-application submission management activities and application requirements or meeting compliance with reporting/data collection requirements, including data calls.
- Development of operating plans for information collection and processing necessary to respond to DHS data calls.
- Travel expenses.
- Meeting-related expenses (For a complete list of allowable meeting-related expenses, please review the 44 CFR.
- Acquisition of authorized office equipment, including personal computers or laptops.

B. Unallowable Costs

Specific unallowable costs include:

- 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.
- Personnel costs (except as detailed above).
- Activities unrelated to the completion and implementation of the FRSGP.
- Other items not in accordance with the Authorized Equipment List or previously listed as allowable costs.

Appendix C

Grants.Gov Quick-Start Instructions

DHS participates in the Bush Administration's e-government initiative. As part of that initiative, all applicants must file their applications using the Administration's common electronic "storefront" -- [grants.gov](http://www.grants.gov). Eligible SAAs must apply for funding through this portal, accessible on the Internet at <http://www.grants.gov>.

Application attachments submitted via [grants.gov](http://www.grants.gov) must be in one of the following formats: Microsoft Word (*.doc), PDF (*.pdf), or text (*.txt). Use the Catalog of Federal Domestic Assistance (CFDA) number listed in the relevant program guidance section of this document in [grants.gov](http://www.grants.gov).

This Appendix is intended to provide guidance on the various steps and activities associated with filing an application using [grants.gov](http://www.grants.gov).

Step 1: Registering.

Registering with [grants.gov](http://www.grants.gov) is a one-time process; however, if you are a first time registrant **it could take 3-5 business days to have your registration validated, confirmed, and receive your user name and password**. It is highly recommended you start the registration process as early as possible to prevent delays in submitting your application package to our agency by the deadline specified. While your registration is pending, you may continue with steps 2, 3, and 4 of these instructions. Registration must be complete for you to be able to submit (step 5) and track (step 6) an application.

1. Establishing an e-business point of contact. [grants.gov](http://www.grants.gov) requires an organization to first be registered in the CCR before beginning the [grants.gov](http://www.grants.gov) registration process. If you plan to authorize representatives of your organization to submit grant applications through [grants.gov](http://www.grants.gov), proceed with the following steps. If you plan to submit a grant application yourself and sign grant applications and provide the required certifications and/or assurances necessary to fulfill the requirements of the application process, proceed to DUNS Number and then skip to the Authorized Organization Representative and Individuals section.

Go to www.grants.gov, and click on the "Get Started" tab at the top of the screen.

- Click the "e-Business Point of Contact" option and click the "GO" button on the bottom right of the screen. If you have already registered with [grants.gov](http://www.grants.gov), you may log in and update your profile from this screen.
- To begin the registration process, click the "Register your Organization [Required]" or "Complete Registration Process [Required]" links. You may print a registration checklist by accessing www.grants.gov/assets/OrganizationRegCheck.pdf.

2. DUNS number. You must first request a Data Universal Numbering System number. Click “Step 1. Request a DUNS Number.” If you are applying as an individual, please skip to “Authorized Organization Representative and Individuals.” If you are applying on behalf of an organization that already has a DUNS number, please proceed to “Step 2. Register with Central Contractor Registry (CCR).” You may obtain a DUNS number at no cost by calling the dedicated toll-free DUNS number request line at 1–866–705–5711.

3. Central Contractor Registry. Registering with the CCR, updating or changing your profile could take up to three to five business days to be confirmed and validated. This delay could prevent your application from being submitted by the deadline specified, so you should register or make changes to your profile as early in the process as possible.

Once you have a DUNS number, click on “Step 2. Register with Central Contractor Registry (CCR).” Here you are required to designate an individual as a point of contact. This point of contact is the sole authority for the organization and has the capability of issuing or revoking another individual’s authority to submit grant applications through grants.gov.

A registration worksheet is provided to assist in the CCR registration process at <http://www.ccr.gov>. It is recommended you review the “Tips for registering with the CCR” at the bottom of this template.

- Go to <http://www.ccr.gov> or click on the CCR icon in the middle of the screen to begin the registration process. To see if your organization is already registered, click “Search CCR” at the top left side of the screen. Search entries must be exact to accurately search the database. If your organization is already registered, you can scroll down and see who the e-Business point of contact is for your agency. If your organization is not already registered, return to the CCR home page and click “Start New Registration” at the top left of the screen.
- If you have problems or questions about the CCR registration process, please contact the CCR Assistance Center at (888) 227–2423.
- Once your registration is complete, you will receive an e-mail with a Trading Partner Identification Number (TPIN) and Marketing Partner Identification Number (MPIN) number. You will need the MPIN number to register with grants.gov. If your organization is already registered with the CCR, you will need to obtain the MPIN number from your e-Business POC.

4. Authorize your Organization Representative. Click “Step 3. Authorize your Organization Representative.” Follow steps 1-4. You will need your DUNS + 4 digit number and the MPIN number CCR e-mailed to you.

5. Log in as e-Business Point of Contact. You may now go to “Step 4. Log in as e-Business Point of Contact.” Here you may authorize or revoke the authority of the

Authorized Organization Representative. Once you are logged in, go to Step 2. *Downloading the Application Viewer*, below.

6. Authorized Organization Representative and Individuals. If you plan to submit a grant application as an individual or an Authorized Organization Representative, with authority to sign grant applications and the required certifications and/or assurances necessary to fulfill the requirements of the application process, proceed with the following steps:

- Go to www.grants.gov and click on the “Get Started” tab at the top of the screen.
- Click the “Authorized Organization Representative (AOR)” option and click the “GO” button to the bottom right of the screen. If you are applying as an individual, click the “Individuals” option and click the “GO” button to the bottom right of the screen.
- If you have previously registered as an AOR, you may start searching for this grant opportunity from this page. Otherwise, you must complete the first-time registration by clicking “Complete First-Time Registration [Required].” You also may click on “Review Registration Checklist” and print a checklist for the following steps (see www.grants.gov/assets/AORRegCheck.pdf).
- Individuals may click the “registration checklist” for help in walking through the registration process.

7. Credential Provider. Once you have entered the registration process, you must register with the credential provider, to safeguard the security of your electronic information. You must have your agency’s or individual DUNS + 4 digit number to complete this process. Now, click on “Step 1. Register with a Credential Provider.” Enter your DUNS number and click “Register.” Once you have entered the required information, click the “Submit” button.

If you should need help with this process, please contact the Credential Provider Customer Service at (800) 386–6820. It can take up to 24 hours for your credential provider information to synchronize with *grants.gov*. Attempting to register with *grants.gov* before the synchronization is complete may be unsuccessful.

8. Grants.gov. After completing the credential provider steps above, click “Step 2. Register with *grants.gov*.” Enter the same user name and password used when registering with the credential provider. You will then be asked to provide identifying information and your organization’s DUNS number. After you have completed the registration process, *grants.gov* will notify the e-Business POC for assignment of user privileges.

Complete the “Authorized Organization Representative User Profile” screen and click “Submit.” *Note:* Individuals do not need to continue to the “Organizational Approval” step below.

9. Organization Approval. Prior to submitting a grant application package, you must receive approval to submit on behalf of your organization. This requirement prevents individuals from submitting grant application packages without permission. A notice is automatically sent to your organization's e-Business POC. Then, your e-Business POC approves your request to become an AOR. You may go to <http://www.ccr.gov> to search for your organization and retrieve your e-Business POC contact information.

Once organization approval is complete, you will be able to submit an application and track its status.

Step 2: Downloading the Application Viewer.

You may download the PureEdge Viewer while your registration is in process. You also may download and start completing the application forms in steps 3 and 4 below. This application viewer opens the application package needed to fill out the required forms. The download process can be lengthy if you are accessing the Internet using a dial-up connection.

- From the [grants.gov](http://www.grants.gov) home page, select the "Apply for Grants" tab at the top of the screen.
- Under "Apply Step 1: Download a Grant Application Package and Applications Instructions," click the link for the PureEdge Viewer (<http://www.grants.gov/DownloadViewer>). This window includes information about computer system requirements and instructions for downloading and installation.

If you are a Macintosh user, please read the PureEdge Support for Macintosh white paper available at

www.grants.gov/GrantsGov_UST_Grantee!/SSL!/WebHelp/MacSupportforPureEdge.pdf.

- Scroll down and click on the link to download the PureEdge Viewer (www.grants.gov/PEViewer/ICSViewer602_grants.exe).
- You will be prompted to save the application. Click the "Save" button and the "Save As" window opens. Select the location where you would like to save PureEdge Viewer and click the "Save" button.
- A window appears to show the progress of the download. When the downloading is complete, click to close the dialog box.
- To install the PureEdge Viewer, locate the file on your computer and click to open it. When you are prompted to run the file, click "RUN." Click "Yes" to the prompt to continue with the installation. The ICS InstallShield Wizard extracts the necessary files and takes you to the "Welcome" page.
- Click "Next" to continue.

- Read the license agreement and click “Yes” to accept the agreement and continue the installation process. This takes you to the “Customer Information” screen.
- Enter a User Name and a Company Name in the designated fields and click “Next.”
- The “Choose Destination Location” window prompts you to select the folder in which PureEdge Viewer will be installed. To save the program in the default folder, click “Next.” To select a different folder, click “Browse.” Select the folder in which you would like to save the program, click on “OK,” then click “Next.”
- The next window prompts you to select a program folder. To save program icons in the default folder, click “Next.” To select a different program folder, type a new folder name or select one from the list of existing folders, then click “Next.” Installation will begin.
- When installation is complete, the “InstallShield Wizard Complete” screen will appear. Click “Finish.” This will launch the “ICS Viewer Help Information” window. Review the information and close the window.

Step 3: Downloading an Application Package.

Once you have downloaded the PureEdge Viewer, you may download and view this application package and solicitation instructions.

- From the [grants.gov](https://www.grants.gov) home page, select the “Apply for Grants” tab at the top of the screen.
- Click “Apply Step 1: Download a Grant Application Package and Application Instructions.”
- Enter the CFDA number for this announcement, **97.075**. Then click “Download Package.” This will take you to the “Selected Grants Application for Download” results page.
- To download an application package and its instructions, click the corresponding download link below the “Instructions and Application” column.
- Once you select a grant application, you will be taken to a “Download Opportunity Instructions and Application” screen to confirm that you are downloading the correct application. If you would like to be notified of any changes to this funding opportunity, enter your e-mail address in the corresponding field, then click the “Submit” button.

- After verifying that you have downloaded the correct opportunity information, click the “Download Application Instructions” button. This will open a PDF of this grant solicitation. You may print the solicitation or save it to your computer by clicking either the print icon at the top tool bar or the “File” button on the top tool bar. If you choose to save the file, click on “Save As” and save to the location of your choice.
- Click the “Back” Navigation button to return to the “Download Opportunity Instructions and Application” page. Click the “Download Application Package” button. The application package will open in the PureEdge Viewer.
- Click the “Save” button to save the package on your computer. Because the form is not yet complete, you will see a prompt that one or more fields may be invalid. You will complete these fields in step 4, but for now, select “Yes” to continue. After you click “Yes,” the “Save Form” window will open.
- Save the application package to your desktop until after submission. Select a name and enter it in the “Application Filing Name” field. Once you have submitted the application through grants.gov, you may then move your completed application package to the file location of your choice.
- Click the “Save” button. If you choose, you may now close your Internet browser and complete your application package offline by double clicking the icon on your desktop. You do not have to be connected to the Internet to complete the application package in step 4 below.

Step 4: Completing the Application Package.

This application can be completed entirely offline; however, you will need to log in to grants.gov to submit the application in step 5.

- Locate the application package you saved on your computer. When you open the package, it will be in PureEdge Viewer. You may save your application at any time by clicking on the “Save” button at the top of the screen.
- Enter a name for your application package in the “Application Filing Name” field. This can be a name of your choice.
- Open and complete all the mandatory and optional forms or documents. To complete a form, click to select the form, and then click the “Open” button. When you open a required form, the mandatory fields will be highlighted in yellow. If you enter incomplete information in a mandatory field, you will receive an error message or the field will turn red, indicating a change needs to be made.

- Mandatory forms include the: (1) Application for Federal Assistance (SF-424); (2) Assurances for Non-Construction Programs (SF-424B); and (3) Disclosure of Lobbying Activities (SF-LLL). These forms can also be viewed at <http://apply.grants.gov/agency/FormLinks?family=7>. Other mandatory forms are identified in Section IV.
- When you have completed a form or document, click the “Close Form” button at the top of the page. Your information will automatically be saved.
- Next, click to select the document in the left box entitled “Mandatory Documents.” Click the “=>” button to move the form or document to the “Mandatory Completed Documents for Submission” box to the right.
- Some mandatory documents will require you to upload files from your computer. To attach a document, select the corresponding form and click “Open.” Click the “Add Mandatory Attachment” button to the left. The “Attach File” box will open. Browse your computer to find where your file is located and click “Open.” The name of that file will appear in the yellow field. Once this is complete, if you would like to attach additional files, click on the “Add Optional Attachment” button below the “Add Mandatory Attachment” button.
- An “Attachments” window will open. Click the “Attach” button. Locate the file on your computer that you would like to attach and click the “Open” button. You will return to the “Attach” window. Continue this process until you have attached all the necessary documents. You may attach as many documents as necessary.
- Once you have finished, click the “Done” button. The box next to the “Attach at Least One Optional Other Attachment” will now appear as checked.
- *Note:* the name of these buttons will vary depending on the name of the form you have opened at that time; i.e., Budget Narrative, Other Attachment, and Project Narrative File.
- To exit a form, click the “Close” button. Your information will automatically be saved.

Step 5: Submitting the Application.

Once you have completed all the yellow fields on all the forms and saved the application on your desktop, check the application package for errors. This can be done any time throughout step 4 above and as often as you like.

- When you are ready to submit your final application package, the “Submit” button at the top of your screen will be enabled. This button will not be activated unless all mandatory data fields have been completed. When you are ready to submit your application, click on “Submit.” This will take you to a “Summary” screen.

- If your “Submit” button is not activated, then click the “Check Package for Errors” button at the top of the “Grant Application Package” screen. PureEdge Viewer will start with the first form and scan all the yellow fields to make sure they are complete. The program will prompt you to fix one error at a time as it goes through the scan. Once there are no more errors, the system will allow you to submit your application to grants.gov.
- Review the application summary. If you wish to make changes at this time, click “Exit Application” to return to the application package, where you can make changes to the forms. To submit the application, click the “Sign and Submit Application” button.
- This will take you to a “Login” screen where you will need to enter the user name and password that you used to register with grants.gov in “Step 1: Registering.” Enter your user name and password in the corresponding fields and click “Login.”
- Once authentication is complete, your application will be submitted. Print this confirmation screen for your records. You will receive an e-mail message to confirm that the application has been successfully uploaded into grants.gov. The confirmation e-mail will give you a grants.gov tracking number, which you will need to track the status of your application. The confirmation e-mail will go to the e-Business POC; therefore, if you are submitting on behalf of someone else, be sure the e-Business POC is aware of the submission and that a confirmation e-mail will be sent.
- When finished, click the “Close” button.

Step 6: Tracking the Application.

After your application is submitted, you may track its status through grants.gov. To do this, go to the grants.gov home page at <http://www.grants.gov>. At the very top of the screen, click on the “Applicants” link. Scroll down the “For Applicants” page and click the “Login Here” button. Proceed to login with your user name and password that was used to submit your application package. Click the “Check Application Status” link to the top left of the screen. A list of all the applications you have submitted through grants.gov is produced. There four status messages your application can receive in the system:

- **Validated.** This means your application has been scanned for errors. If no errors were found, it validates that your application has successfully been submitted to grants.gov and is ready for the agency to download your application.
- **Received by Agency.** This means our agency DHS downloaded your application into our electronic Grants Management System (GMS) and your application is going through our validation process to be successfully received on our end.

- **Agency Tracking Number Assigned.** This means our GMS did not find any errors with your package and successfully downloaded your application into our system.
- **Rejected With Errors.** This means your application was either rejected by *grants.gov* or GMS due to errors. You will receive an e-mail from [grants.gov](https://www.grants.gov) customer support, providing details of the results and the next steps required. Most applications are rejected because: (1) a virus was detected; (2) you are using a user name and password that has not yet been authorized by the organization's e-Business POC; or (3) the DUNS number you entered on the SF-424 form does not match the DUNS number that was registered in the CCR for this organization.

If you experience difficulties at any point during this process, please call the [grants.gov](https://www.grants.gov) customer support hotline at 1-800-518-4726.

Appendix D Investment Justification

A. Investment Justification Overview

As part of the FY 2008 FRSGP application process, applicants must develop an Investment Justification that addresses each initiative being proposed for funding. These Investment Justifications must demonstrate how proposed projects assist in conducting vulnerability assessments, developing security plans, or improve/expand training.

Applicants may propose up to two investments within their Investment Justification. A separate Investment Justification must be submitted for each proposed project. All investment justifications must be submitted with the application by March 17, 2008.

The Investment Justification must demonstrate the ability of the applicant to provide tangible, physical security enhancements consistent with the purpose of the program and guidance provided by DHS. Applicants must ensure that the Investment Justification is consistent with all applicable requirements outlined in this application kit. The format attached should be followed for these file attachments.

As a reminder, completed Applications must be submitted to DHS via grants.gov no later than 11:59 pm EDT, March 17, 2008. Systems must submit one SF-424; as well as an investment justification and detailed budget for each project.

B. Investment Justification Template.

Applicants must provide information in the following categories for **each** proposed investment:

1. *Background;*
2. *Impact;*
3. *Implementation Plan.*

FRSGP applicants must provide responses to all questions. The noted page limits are suggestions only.

| Investment Heading | |
|---|----|
| Railroad Carrier | |
| Date of Application | |
| Region and High Population-Density Area(s) Impacted | |
| Investment Name | |
| Investment Amount | \$ |

I. Background

Note: This section only needs to be completed once per application, regardless of the number of investments proposed. The information in this section provides background/context for the investment(s) requested, but does not represent the evaluation criteria used by DHS for rating individual investment proposals.

| I.A. Identify the point(s) of contact for this investment. | |
|--|---|
| Response Type | Narrative |
| Page Limit | Not to exceed ½ page |
| Response Instructions | Identify the following: <ul style="list-style-type: none"> • Point of contact's (POC) name and title; • POC's full mailing address; • POC's telephone number; • POC's fax number; • POC's email address; and, • Also include the corresponding information for the single authorizing official for your organization—i.e., the individual authorized to sign a grant award. |
| Response: | |

| I.B. Describe your operating system. | |
|---|---|
| Response Type | Narrative |
| Page Limit | Not to exceed 2 pages |
| Response Instructions | Describe the following: <ul style="list-style-type: none"> • Infrastructure; • Number of track miles; • Number of rail cars (differentiating tank cars); • Volume of SSM as defined for this grant, transported through High Population-Density Areas annually. (Include separately the volume of TIH transported in tank cars and the volume of TIH transported by bulk loads.) • System maps, including listing of High Density Population Areas serviced; and, • Other sources of funding being leveraged for security enhancements. |
| Response | |

| I.C. Describe the status of your training program. | |
|---|--|
| Response Type | Narrative |
| Page Limit | Not to exceed 2 pages |
| Response Instructions | Describe the following: <ul style="list-style-type: none"> • Number of staff • Type of staff, including employment titles • The number of employees who have received basic security awareness training in the past two years |
| Response | |

II. Impact

| II.A. Discuss how the implementation of this investment will decrease or mitigate risk. | |
|---|---|
| Response Type | Narrative |
| Page Limit | Not to exceed 1 page |
| Response Instructions | <ul style="list-style-type: none"> • Discuss how this investment will reduce risk (e.g., reduce vulnerabilities or mitigate the consequences of an event) by addressing the needs and priorities identified in earlier analysis and review; and, • Identify the nature of the risk and how the risk and need are related to show how addressing the need through this investment will also mitigate risk (e.g., reduce vulnerabilities or mitigate the consequences of an event). • For training requests, provide how close the training request will get your organization to having all railroad frontline employees trained for basic security training. Also please explain your plan for getting everyone trained in basic security. |
| Response | |

| II.B. Vulnerability assessments and security plan requests. | |
|---|--|
| Response Type | Narrative |
| Page Limit | Not to exceed 2 pages |
| Response Instructions | <p>For vulnerability assessment and security plan requests, please explain the status of your current vulnerability assessment and security plan with regard to the requirements detailed in Appendix E (Vulnerability Assessment) and Appendix F (Security Plan). If you deem your current vulnerability assessment and security plan do not meet the requirements contained herein, please describe those aspects of the plan that will be created and/or improved with grant funds.</p> <ul style="list-style-type: none"> • If using a vulnerability tool/methodology other than those identified in Section C of Appendix E, you must request provide the commercial name of the assessment tool/methodology in the response to facilitate evaluation of your proposed methodology; • If it is not a commercial product, explain why you are not using one of the approved methodologies and how your chosen methodology will comply with the outlines in Appendices E and/or F; • DHS may require the applicant to submit the entire vulnerability assessment tool/methodology requested above; |
| Response | |

III. Funding and Implementation Plan

| III.A. Investment Funding Plan. | |
|---------------------------------|--|
| Response Type | Numeric and Narrative |
| Page Limit | Not to exceed 1 page |
| Response Instructions | <ul style="list-style-type: none"> • Complete the chart below to identify the amount of funding you are requesting for <u>this Investment only</u>; • Funds should be requested by allowable cost categories (as identified in the FY 2008 FRSGP Program Guidelines and Application Kit); • Applicants must make funding requests that are reasonable and justified by direct linkages to activities outlined in this particular Investment; and, • Applicants must indicate whether additional funding (non-FY 2008 FRSGP) will be leveraged for this Investment. <p>Note: Investments will be evaluated on the expected impact on security relative to the amount of the investment (i.e., cost effectiveness). An itemized Budget Detail Worksheet and Budget Narrative must also be completed for this investment. See Appendix H of this document for a sample format.</p> |
| Response | |

The following template illustrates how the applicants should indicate the amount of FY 2008 FRSGP funding required for the Investment, how these funds will be allocated across the cost elements, and any match being offered:

| | FY 2008 FRSGP Request Total | Match | Grand Total |
|--|-----------------------------|-------|-------------|
| <i>Vulnerability Assessment/ Security Plan Development</i> | | | |
| <i>Training</i> | | | |
| <i>M&A</i> | | | |
| Total | | | |

| III.B. Identify up to five potential challenges to the effective implementation of this investment (e.g., stakeholder buy-in, sustainability, aggressive timelines). | |
|---|---|
| Response Type | Narrative |
| Page Limit | Not to exceed ½ page |
| Response Instructions | <ul style="list-style-type: none"> • For each identified challenge, provide a brief description of how the challenge will be addressed and mitigated, and indicate a probability of occurrence (high, medium, or low); • The response should focus on the implementation only; • Consider the necessary steps and stages that will be required for successful implementation of the investment; • Identify areas of possible concern or potential pitfalls in terms of investment implementation; and, • Explain why those areas present the greatest challenge to a successful investment implementation. |
| Response | |

| III.C. Describe the management team, including roles and responsibilities, that will be accountable for the oversight and implementation of this investment, and the overall management approach they will apply for the implementation of this investment. | |
|--|--|
| Response Type | Narrative |
| Page Limit | Not to exceed ½ page |
| Response Instructions | <ul style="list-style-type: none"> • Provide the high-level skill sets (e.g., budget execution, grant administration, geospatial expert, outreach and communication liaison) that members of the management team must possess for the successful implementation and oversight of the investment; • Discuss how those skill sets fulfill the oversight and execution responsibilities for the investment, and how the management roles and responsibilities will be distributed/assigned among the management team; and, • Explain how the management team members will organize and work together in order to successfully manage the investment. |
| Response | |

| | |
|--|---|
| III.D. Provide a high-level timeline, milestones and dates, for the implementation of this investment. Possible areas for inclusion are: stakeholder engagement, planning, major acquisitions/purchases, training, exercises, and process/policy updates. <u>Up to 10</u> milestones may be provided. | |
| Response Type | Narrative |
| Page Limit | Not to exceed 1 page |
| Response Instructions | <ul style="list-style-type: none"> Only include major milestones that are critical to the success of the investment; While up to 10 milestones may be provided, applicants should only list as many milestones as necessary; Milestones are for this discrete investment – those that are covered by the requested FY 2008 FRSGP funds and will be completed over the 36-month grant period; Milestones should be kept to high-level, major tasks that will need to occur; Identify the planned start date associated with the identified milestone. The start date should reflect the date at which the earliest action will be taken to start achieving the milestone; Identify the planned completion date when all actions related to the milestone will be completed and overall milestone outcome is met; and, List any relevant information that will be critical to the successful completion of the milestone (such as those examples listed in the question text above). |
| Response | |

C. Investment Justification Submission and File Naming Convention

Investment Justifications must be submitted with the grant application as a file attachment within grants.gov. Applicants must use the following file naming convention when submitting the Investment Justifications as part of the FY 2008 FRSGP:

Investment Justification (through grants.gov file attachment)

Name of Applicant_ IJ Number (Example: ABC Freight Carrier_IJ_#1)

Appendix E

Vulnerability Assessment

A. Vulnerability Assessment Overview

Each railroad carrier must complete a Vulnerability Assessment of all railroad carrier critical assets and infrastructure, and the carrier's transportation and storage of SSM in rail cars, excluding residue.

B. Vulnerability Assessment Structure

A rail carrier Vulnerability Assessment shall include:

1. The identification of all railroad carrier critical assets and infrastructure needed to conduct railroad operations including intermodal terminals, tunnels, bridges, switching and storage areas, SSM transported by the railroad carrier and information systems as appropriate.
2. Each asset should be assessed as the target of at least the following acts of terrorism (attack scenarios): a VBIED attack, an IED attack, and a cyber attack (if applicable). Additional attack scenarios should be assessed if applicable.
3. The identification of the vulnerabilities of the identified critical railroad assets and infrastructure to each applicable act of terrorism including the identification of strengths and weaknesses and the existing countermeasures and their level of effectiveness in reducing identified vulnerabilities taking into account the following:
 - a. Physical security including fencing, alarms, monitoring using cameras and patrols, warning signs and lighting;
 - b. Randomness of operations;
 - c. Access control of employees, contractors, visitors and trespassers to critical areas;
 - d. Programmable electronic devices, computers, or other automated systems which are used in providing the transportation;
 - e. Communications systems and utilities needed for railroad security purposes including dispatching and notification systems;
 - f. Planning including the coordination with the public emergency responders and law enforcement agencies;
 - g. Employee and contractor personnel screening;
 - h. Employee security training, and;
 - i. Dwell time of rail cars containing SSM cars in rail yards, terminals, and on railroad-controlled leased track.

4. The identification of redundant and backup systems required to provide for the continued operation of critical elements of a railroad carrier's system in the event of an act of terrorism, including disruption of commercial electric power or communications network.
5. An analysis of the consequences of each applicable act of terrorism on the identified critical assets. This includes estimating the impact the act of terrorism will have on railroad operations, the population, national security, and the national economy.
6. A risk assessment for each identified critical railroad carrier asset and infrastructure that takes into account the relative degree of risk in terms of the consequences of the act of terrorism and the likelihood of a success of the act of terrorism and threat information available to the rail carrier.

C. Vulnerability Assessment Methodologies

The rail carrier vulnerability assessment must be conducted using a tool or methods which meets the above criteria and must be accepted by DHS/TSA.

Some examples of the publicly available methodologies that meet these criteria include but are not limited to the DHS Transit Risk Assessment Module (TRAM) and the Intelligence Community's Analytical Risk Management (ARM) Process. Various commercially available tools meet these criteria.

Applicants should send an email to TSAGrants@tsa.dhs.gov for additional information.

Appendix F Security Plan

A. Security Plan Overview

The security plan must be based on and supported by the railroad carrier's vulnerability assessment. The security plan ensures that security processes and procedures are in place to effectively prevent and respond to threat incidents and terrorist attacks.

B. Freight Rail Security Plan Structure

1. Elements of the Security Plan. The Plan should address the following elements, as applicable:

- a. Rail Carrier's Statement of Security Plan Objectives (what the plan sets out to do).
- b. Designation of "Rail Security Coordinator(s)"—Team responsible for developing, managing, and ensuring the security countermeasures are implemented during raised alert levels or response to a security threat/incident.
- c. Roles and Responsibilities of those designated with security responsibilities.
- d. Procedures in place to communicate, disseminate, and respond to threat information.
- e. Procedures for updating information and ensuring security countermeasures are being implemented during raised alert levels (Process needs to be set up to get the latest information internally and to be able to externally communicate the status of their security response related to a terrorist attack or security incident).
- f. Security countermeasures to be implemented by your railroad in response to a terrorist attack or threat incident at each alert level (blue to red).
- g. Procedures in place for periodic audits, exercises and drills for security plans, and for its amendment in response to experience.
- h. Measures to prevent unauthorized access to designated or restricted areas.
- i. Measures to prevent the introduction of dangerous substances and devices to designated restricted areas and/or railroad property.
- j. Procedures and expected timeframes for responding to security threats or breaches of security, including provisions for maintaining security of infrastructure and operations on railroad property.

- k. Identifications of security processes to work with State and local law enforcement agencies, emergency responders, and Federal officials in response to a terrorist attack.
- l. Procedures for evacuating railroad facilities or conveyances in case of reliable security threats or breaches of security.
- m. Procedures in place for protection of railroad carrier designated critical infrastructures.
- n. Procedures for employee identification and background checks for employees and contractors.
- o. Identification of, and methods to communicate with railroad, system and facility security officers, company security officers, field operating and security officers and management personnel, public safety officers and emergency response personnel, crisis management organizational representatives in local areas, including 24 hour contact details.
- p. Security measures designed to ensure security of local communities, critical infrastructure, special events, railroad facilities, railroad conveyances/equipment, passengers and passenger trains operating on railroad tracks owned or operated by your railroad, cargo and cargo handling equipment owned by you or your customer and other railroad interdependencies covered contractual agreements.
- q. Procedures to address handling and storage of toxic inhalation hazardous materials.
- r. Plan for employee security awareness training to include timeline for conducting employee training.
- s. Plans and procedures to provide redundant and backup systems required to ensure continued railroad operations.
- t. Procedures to respond to and facilitate the recovery of the railroad operations after a transportation security incident.
- u. Procedures for cyber security.
- v. Appendix containing risk mitigation strategies for addressing vulnerabilities identified in the vulnerability assessment but not sufficiently addressed by the security plan. This should include:
 - (1) Outstanding vulnerabilities
 - (2) Mitigation options and associated costs of alternatives
 - (3) Preferred mitigation strategy
 - (4) Comprehensive funding plan and schedule for risk remediation

Appendix G

Frontline Employee Security Training

A. Training Overview

A robust security training program includes the following components for training of ***railroad frontline employees, as appropriate:***

1. Security Awareness
 - a. Identifying, reporting, and reacting to suspicious activity, suspicious items, dangerous substances, and security incidents;
 - b. Determining the seriousness of an occurrence or threat; and
 - c. Recognizing the characteristics of improvised explosive devices (IED) and weapons of mass destruction (WMD) and reporting and reacting to these threats in the confines of trains and critical infrastructure.
2. Behavior Recognition
 - a. Recognizing behaviors associated with terrorists' reconnaissance and planning activities; and
 - b. Behavioral and psychological aspects of, and responses to, terrorist incidents, including the ability to cope with hijacker behavior.
3. Threat/Incident Prevention, Protection, and Response
 - a. Understanding individual roles and responsibilities in prevention of and response to terrorist attacks;
 - b. Crew communication and coordination;
 - c. Evacuation procedures for employees;
 - d. Self defense and use of non-lethal defense devices;
 - e. Use of personal protective devices and other protective equipment;
 - f. Procedures for communicating and interacting with governmental and nongovernmental emergency response providers;
 - g. Operation and maintenance of security equipment and systems, to the extent the employee's responsibilities involve use or maintenance of such equipment; and
 - h. Live situational exercises regarding various threat conditions.

In addition to meeting the criteria listed under "Security Awareness" and "Behavior Recognition" above, ***operations control center/operations dispatch center personnel*** should address the following adjusted components:

1. Threat/Incident Prevention, Protection, and Response

- a. Understanding the role of the operations control center in the prevention of, protection against and response to terrorist attacks;
- b. Implementing freight rail carrier's security and emergency management plans, including prevention, protection, and response activities for threats or incidents involving improvised explosive devices and weapons of mass destruction;
- c. Understanding individual roles and responsibilities in prevention of, protection against and response to terrorist attacks and the railroad carrier's role in terrorism-related incidents in the broader community;
- d. Specifying priorities in prevention of, protection against, and response to a terrorist threat or attack;
- e. Directing and coordinating prevention, protection and response activities for terrorist threat or attack;
- f. Ensuring effective command and control of and communications among law enforcement agencies, fire services, emergency medical services, and other entities providing security augmentation or emergency response;
- g. Use of personal protective devices and other protective equipment;
- h. Procedures for communicating and interacting with governmental and nongovernmental emergency response providers;
- i. Operation and maintenance of security equipment and systems, to the extent the employee's responsibilities involve use or maintenance of such equipment; and
- j. Table top and live situational exercises testing capabilities to direct and coordinate prevention and response activities for terrorist threats or attacks.

B. Available Training

DHS has identified different allowable types of training ("Basic" and "Follow-On"), employee categories, and course duration, as well as indications of what types of employees should receive what types of training for the FY 2008 FRSGP.

Training courses must be DHS-approved courses. For areas where there are no identified courses, eligible railroad carriers are encouraged to develop their own training programs, or see which other emergency management courses already offered may be adapted to cover this subject area.

The vendors providing training do not necessarily need to be DHS-approved vendors. If for some reason applicants are having difficulties scheduling the training with an

approved vendor, or no approved vendors have been identified, applicants may identify other vendors to provide the training. However, DHS must be notified prior to conducting the training.

Training must be completed within the 36-month grant period of performance.

| Training Description | Focus | Categories of Employees to Receive | | |
|--|--|------------------------------------|--------------------------------------|--|
| | | Front-Line Employees | Operations Dispatch Center Personnel | Direct Supervisors of Front Line Employees |
| Security Awareness | Enhance capability to identify, report, and react to suspicious activity, suspicious items, dangerous substances, and security incidents. | | | |
| Behavior Recognition | Recognize behaviors associated with terrorists' reconnaissance and planning activities and behavioral and psychological aspects of, and responses to, terrorist incidents, including the ability to cope with hijacker behavior. | | | |
| Threat/Incident Prevention, Protection and Response | Understanding individual roles and responsibilities in prevention of and response to terrorist attacks. | | | |
| Operations Control Center/Dispatch Center Readiness | Determining the seriousness of an occurrence or threat; and understanding and differentiating the characteristics of improvised explosive devices (IED) and weapons of mass destruction (WMD) and reporting and reacting to these threats in the confines of trains, as appropriate for the service provided, and system infrastructure. | | | |

| FREIGHT RAIL SECURITY FOLLOW-ON COURSES | | | | |
|--|--|-------------------------------|--------------------------------------|----------------------|
| Training Description | Focus | Railroad Front-Line Employees | Operations Dispatch Center Personnel | Mid-Level Management |
| <i>What is Security? (NTI at Rutgers University Training Video Module 1)</i> | Ensure employees throughout the freight rail industry understand their individual roles in knowing when something is not right and how to take the initiative to report it to the proper authorities. | | | |
| <i>Vulnerability and Risk (NTI at Rutgers University Training Video Module 3)</i> | Ensure employees throughout the freight rail industry understand the importance of maintaining vigilance to reduce the risk of becoming vulnerable to terrorism and how to continue efforts to eliminate exposure. | | | |
| <i>What to Look for (NTI at Rutgers University Training Video Module 4)</i> | Employees throughout the freight rail industry will learn important facets of securing the railroad. | | | |
| <i>Your Role (NTI at Rutgers University Training Video Module 2)</i> | Enable freight railroad employees to focus on what can be done to enhance security by providing key elements to provide a more secure workplace. | | | |
| <i>Security Awareness/Improvised Explosive Device Video (TSA Video)</i> | Instruct freight railroad employees on how to identify, describe, and report to proper officials the location of an IED when detected. | | | |

Appendix H Sample Budget Detail Worksheet

OMB Approval No. 1121-0188

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

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

| <u>Name/Position</u> | <u>Computation</u> | <u>Cost</u> |
|----------------------|--------------------|-------------|
|----------------------|--------------------|-------------|

Note: Personnel costs are only allowable for direct management and administration of the grant award, i.e., preparation of mandatory post-award reports.

TOTAL _____

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

| <u>Name/Position</u> | <u>Computation</u> | <u>Cost</u> |
|----------------------|--------------------|-------------|
|----------------------|--------------------|-------------|

TOTAL _____

Total Personnel & Fringe Benefits _____

C. Equipment. List non-expendable items that are to be purchased. Non-expendable equipment is tangible property having a useful life of more than two years. (Note: Organization’s own capitalization policy and threshold amount for classification of equipment may be used). Expendable items should be included either in the “Supplies” category or in the “Other” category. Applicants should analyze the cost benefits of purchasing versus leasing equipment, especially high cost items and those subject to

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

Item **Cost**

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

Subtotal _____

TOTAL _____

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

Description **Computation** **Cost**

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

Important Note: If applicable to the project, construction costs should be included in this section of the Budget Detail Worksheet.

TOTAL _____

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

Description **Computation** **Cost**

TOTAL _____

Budget Summary. When you have completed the budget worksheet, transfer the totals for each category to the spaces below. Compute the total direct costs and the

total project costs. Indicate the amount of Federal funds requested and the amount of non-Federal funds that will support the project.

| <u>Budget Category</u> | <u>Federal Amount</u> | <u>Non-Federal Amount</u> |
|----------------------------------|-----------------------|---------------------------|
| A. Personnel | _____ | _____ |
| B. Fringe Benefits | _____ | _____ |
| C. Equipment | _____ | _____ |
| D. Supplies | _____ | _____ |
| E. Consultants/Contracts | _____ | _____ |
| F. Other | _____ | _____ |
| Total Direct Costs | _____ | _____ |
| G. Indirect Costs | _____ | _____ |
| * TOTAL PROJECT COSTS | _____ | _____ |
| Federal Request | _____ | |
| Non-Federal Amount (Cost Share)) | _____ | |

Detailed Budget Submission and File Naming Convention

Detailed Budgets must be submitted with the grant application as a file attachment within grants.gov. Applicants must use the following file naming convention when submitting required documents as part of the FY 2008 FRSGP.

Detailed Budget (through Grants.gov file attachment)

- Name of Applicant_ IJ Number_Budget (Example: ABC Freight Railroad Carrier_IJ#1_Budget)

Appendix I

Award and Reporting Requirements

Prior to the transition to FEMA, the former Office of Grants and Training preparedness programs followed The Department of Justice's codified regulations, 28 CFR and the OGO Financial Management Guide. The former Office of Grants and Training is now within FEMA and all preparedness programs will follow FEMA's codified regulations, 44 CFR.

A. Grant Award and Obligation of Funds.

Upon approval of an application, the grant will be awarded to the grant recipient. The date that this is done is the “award date.”

Obligations are a legal liability to pay, under a grant, subgrant, or contract, determinable sums for services or goods incurred during the grant period. This includes, but is not limited to, amounts of orders placed, contracts and subgrants awarded, goods and services received, and similar transactions during a given period that will require payment by the grantee during the same or a future period.

The period of performance is 36 months. Any unobligated funds will be deobligated at the end of this period. Extensions to the period of performance will be considered only through formal requests to FEMA with specific and compelling justifications why an extension is required.

B. Post Award Instructions.

The following is provided as a guide for the administration of an award. Additional details and requirements may be provided to the grantee in conjunction with finalizing an award.

1. Review award and special conditions document. Notification of award approval is made by e-mail through the Grants Management System (GMS). Once an award has been approved, a notice is sent to the e-mail address of the individual who filed the application, as well as to the authorized grantee official. Follow the directions in the notification e-mail and log into GMS to access the award documents. The authorized grantee official should carefully read the award and special condition documents. If you do not receive a notification e-mail, please contact your Preparedness Officer for your award number. Once you have the award number, contact the GMS Help Desk at (888) 549-9901, option 3 to obtain the username and password associated with the new award.

If you agree with the terms and conditions, the authorized grantee official should sign and date both the original and the copy of the award document page in Block 19 and initial the special conditions page(s). Retain a copy and fax the documents to (202) 786-9905 Attention: Control Desk or send the original signed documents to:

**U.S. Department of Homeland Security/FEMA
Grant Programs Directorate/Control Desk 4th Floor, TechWorld
500 C St SW
Washington, DC 20472**

If you do not agree with the terms and conditions, contact the Preparedness Officer named in the award package.

2. Complete and return form SF1199A . The SF1199A Direct Deposit Sign-up Form is used to set up direct deposit for grant payments. The SF1199A form can be found at: <http://www.fema.gov/government/grant/administration.shtm>.

NOTE: Please include your vendor number in Box C of the SF1199A form.

3 Access to payment systems. Grantees under this solicitation will use FEMA's online Payment and Reporting System (PARS) to request funds. The website to access PARS is <https://isource.fema.gov/sf269/execute/Login?sawContentMessage=true>. Questions regarding payments or how to access PARS should be directed to the FEMA Call Center at (866) 927-5646 or sent via e-mail to ask-OGO@dhs.gov.

4. Reporting requirements. Reporting requirements must be met throughout the life of the grant (refer to the program guidance and the special conditions found in the award package for a full explanation of these requirements. Please note that PARS contains edits that will prevent access to funds if reporting requirements are not met on a timely basis.

5. Questions about your award? A reference sheet is provided containing frequently asked financial questions and answers. Financial management questions regarding your award should be directed to the FEMA Call Center at (866) 927-5646 or sent via e-mail to ask-OGO@dhs.gov.

Note: If you have any questions about GMS, need to establish a GMS account, or require technical assistance with accessing your award, please contact the GMS Help Desk at (888) 549-9901.

C. Drawdown and Expenditure of Funds.

Following acceptance of the grant award and release of any special conditions withholding funds, the grantee can drawdown and expend grant funds through PARS.

Grant recipients should request funds based upon immediate disbursement requirements. Funds will not be paid in a lump sum, but rather disbursed over time as project costs are incurred or anticipated. Recipients should time their drawdown requests to ensure that Federal cash on hand is the minimum needed for disbursements to be made immediately or within a few days. Grantees may elect to

draw down funds up to 120 days prior to expenditure/ disbursement. FEMA strongly encourages recipients to draw down funds as close to expenditure as possible to avoid accruing interest.

Funds received by grantees must be placed in an interest-bearing account and are subject to the rules outlined in 44 CFR Part 13, Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments and 2 CFR Part 215, Uniform Administrative Requirements for Grants and Agreements (Including Sub-awards) with Institutions of Higher Education, Hospitals and other Non-profit Organizations (formerly OMB Circular A-110). These regulations further provide that entities are required to promptly, but at least quarterly, remit interest earned on advances to:

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

The grantee may keep interest earned, up to \$100 per fiscal year for administrative expenses. This maximum limit is not per award; it is inclusive of all interest earned on all Federal grant program funds received.

Although advance drawdown requests are permissible, State grantees remain 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 for program purposes.

D. Reporting Requirements.

1. Financial Status Report (FSR) -- required quarterly. Obligations and expenditures must be reported on a quarterly basis through the FSR, which is due within 30 days of the end of each calendar quarter (e.g., for the quarter ending March 31, FSR is due no later than April 30). A report must be submitted for every quarter of the period of performance, including partial calendar quarters, as well as for periods where no grant activity occurs. Future awards and fund draw downs may be withheld if these reports are delinquent. The final FSR is due 90 days after the end date of the performance period.

FSRs **must be filed online** through the PARS.

Required submission: Financial Status Report (FSR) SF-269a (due quarterly).

2. Categorical Assistance Progress Report (CAPR). Following an award, the awardees will be responsible for providing updated obligation and expenditure information on a semi-annual basis. The CAPR is due within 30 days after the end of the reporting period (July 30 for the

reporting period of January 1 through June 30, and on January 30 for the reporting period of July 1 through December 31). Future awards and fund drawdowns may be withheld if these reports are delinquent. The final CAPR is due 90 days after the end date of the performance period.

Block #12 of the CAPR should be used to note progress against the proposed project. The grantor agency shall provide sufficient information to monitor program implementation and goal achievement. At a minimum, reports should contain the following data: (1) As applicable, the total number of items secured under this grant (e.g., access controls, surveillance, physical enhancements, and vessels) to date, and (2) for other items acquired through this grant, a brief description and total number of items obtained to date.

CAPRs must be filed online through the internet at: <https://grants.ojp.usdoj.gov>. Guidance and instructions can be found at: <https://grants.ojp.usdoj.gov/gmsHelp/index.html>.

Required submission: BSIR and CAPR (due semi-annually).

3. Exercise Evaluation and Improvement. Exercises implemented with grant funds should be threat- and performance- based and should evaluate performance of critical prevention and response tasks required to respond to the exercise scenario. Guidance on conducting exercise evaluations and implementing improvement is defined in the *Homeland Security Exercise and Evaluation Program (HSEEP) Volume II: Exercise Evaluation and Improvement* located at <http://www.hseep.dhs.gov>. Grant recipients must report on scheduled exercises and ensure that an After Action Report (AAR) and Improvement Plan (IP) are prepared for each exercise conducted with FEMA support (grant funds or direct support) and submitted to FEMA within 60 days following completion of the exercise.

The AAR documents the performance of exercise related tasks and makes recommendations for improvements. The IP outlines the actions that the exercising jurisdiction(s) plans to take to address recommendations contained in the AAR. Generally the IP, with at least initial action steps, should be included in the final AAR. FEMA is establishing a national database to facilitate the scheduling of exercises, the submission of the AAR/IPs and the tracking of IP implementation. Guidance on the development of AARs and IPs is provided in Volume II of the HSEEP manuals.

Required submissions: AARs and IPs (as applicable).

4. Financial and Compliance Audit Report. Recipients that expend \$500,000 or more of Federal funds during their fiscal year are required to submit an organization-wide financial and compliance audit report. The audit must be performed in accordance with the U.S. General Accountability Office, *Government Auditing Standards*, located at <http://www.gao.gov/govaud/ybk01.htm>, and *OMB Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations*, located at <http://www.whitehouse.gov/omb/circulars/a133/a133.html>. Audit reports are currently due to the Federal Audit Clearinghouse no later than nine months after the end of the recipient's fiscal year. In addition, the Secretary of Homeland Security and the

Comptroller General of the United States shall have access to any books, documents, and records of recipients of grants assistance for audit and examination purposes, provided that, in the opinion of the Secretary or the Comptroller, these documents are related to the receipt or use of such assistance. The grantee will also give the sponsoring agency or the Comptroller, 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-grantees 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.

5. Federal Funding Accountability and Transparency Act. While there are no State and Urban Area requirements in FY 2008, the Federal Funding Accountability and Transparency Act of 2006 may affect State and Urban Area reporting requirements in future years. The Act requires the Federal government to create a publicly searchable online database of Federal grant recipients by January 1, 2008 with an expansion to include sub-grantee information by January 1, 2009.

6. National Preparedness Reporting Compliance. The Government Performance and Results Act (GPRA) requires that the Department collect and report performance information on all programs. For grant programs, the prioritized Investment Justifications and their associated milestones provide an important tool for assessing grant performance and complying with these national preparedness reporting requirements. FEMA will work with grantees to develop tools and processes to support this requirement. DHS anticipates using this information to inform future-year grant program funding decisions.

7. State Preparedness Report. Congress requires that States receiving DHS-administered Federal preparedness assistance shall submit a State Preparedness Report to the Department on the State's level of preparedness by March 31, 2008, and annually thereafter. The report shall include: (1) an assessment of State compliance with the national preparedness system, NIMS, the NRP, and other related plans and strategies; (2) an assessment of current capability levels and a description of target capability levels; and (3) an assessment of resource needs to meet the National Preparedness Priorities, including an estimate of the amount of expenditures required to attain the Priorities and the extent to which the use of Federal assistance during the preceding fiscal year achieved the Priorities.

E. Monitoring.

Grant recipients will be monitored periodically by FEMA staff, both programmatically and financially, to ensure that the project goals, objectives, performance requirements, timelines, milestone completion, budgets and other related program criteria are being met. Monitoring will be accomplished through a combination of office-based reviews and on-site monitoring visits. Monitoring will involve the review and analysis of the financial, programmatic, performance and administrative issues relative to each

program and will identify areas where technical assistance and other support may be needed.

The recipient is responsible for monitoring award activities, to include sub-awards, to provide reasonable assurance that the Federal award is administered in compliance with requirements. Responsibilities include the accounting of receipts and expenditures, cash management, maintaining of adequate financial records, and refunding expenditures disallowed by audits.

F. Grant Close-Out Process.

Within 90 days after the end of the award period, grantees must submit a final FSR and final CAPR detailing all accomplishments throughout the project. After these reports have been reviewed and approved by FEMA, 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 deobligated, 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 GPD, the grant will be identified as “Closed by the Grant Programs Directorate.”

Required submissions: (1) final SF-269a, due 90 days from end of grant period; and (2) final CAPR, due 90 days from the end of the grant period.

Appendix J

Additional Resources

This Appendix describes several resources that may help applicants in completing a FRSGP application.

1. Centralized Scheduling & Information Desk (CSID) Help Line. The CSID is a non-emergency resource for use by emergency responders across the nation. CSID is a comprehensive coordination, management, information, and scheduling tool developed by DHS through FEMA for homeland security terrorism preparedness activities. The CSID provides general information on all FEMA preparedness grant programs and information on the characteristics of CBRNE, agro-terrorism, defensive equipment, mitigation techniques, and available Federal assets and resources.

The CSID maintains a comprehensive database containing key personnel contact information for homeland security terrorism preparedness programs and events. These contacts include personnel at the Federal, State and local levels. The CSID can be contacted at (800) 368-6498 or askcsid@dhs.gov. CSID hours of operation are from 8:00 am–6:00 pm (EST), Monday-Friday.

2. Grant Programs Directorate (GPD). FEMA GPD will provide fiscal support, including pre- and post-award administration and technical assistance, to the grant programs included in this solicitation.

For financial and administrative guidance, all state and local government grant recipients should refer to 44 CFR Part 13, Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments. Institutions of higher education, hospitals, and other non-profit organizations should refer to 2 CFR Part 215 for the applicable uniform administrative requirements.

Additional guidance and information can be obtained by contacting the FEMA Call Center at (866) 927-5646 or via e-mail to ask-OGO@dhs.gov.

3. GSA's Cooperative Purchasing Program. The U.S. General Services Administration (GSA) offers two efficient and effective procurement programs for State and local governments to purchase products and services to fulfill homeland security and other technology needs. The GSA Schedules (also referred to as the Multiple Award Schedules and the Federal Supply Schedules) are long-term, indefinite delivery, indefinite quantity, government-wide contracts with commercial firms of all sizes.

- Cooperative Purchasing Program
Section 211 of the E-Government Act of 2002, authorized GSA sales of Schedule 70 IT products and services to State and Local Governments through the introduction of Cooperative Purchasing. The Cooperative Purchasing program allows State and local governments to purchase from Schedule 70 (the Information Technology Schedule) and the Consolidated Schedule (containing IT Special Item Numbers) **only**. Cooperative

Purchasing is authorized by Federal law and was enacted when Section 211 of the E-Government Act of 2002 amended the Federal Property and Administrative Services Act.



Under this program, State and local governments have access to over 3,500 GSA Schedule contractors who have voluntarily modified their contracts to participate in the Cooperative Purchasing program. The U.S. General Services Administration provides a definition of State and local governments as well as other vital information under the frequently asked questions section on its website at <http://www.gsa.gov/cooperativepurchasing>.

- **Disaster Recovery Purchasing Program**

GSA plays a critical role in providing disaster recovery products and services to Federal agencies. Now State and Local Governments can also benefit from the speed and savings of the GSA Federal Supply Schedules. Section 833 of the John Warner National Defense Authorization Act for Fiscal Year 2007 (Public Law 109-364) amends 40 U.S.C. 502 to authorize the GSA to provide State and Local governments the use of ALL Federal Supply Schedules of the GSA for purchase of products and services to be used to *facilitate recovery from a major disaster declared by the President under the Robert T. Stafford Disaster Relief and Emergency Assistance Act or to facilitate **recovery** from terrorism or nuclear, biological, chemical, or radiological attack.*

In the aftermath of emergency events, State or local governments' systems may be disrupted. Thus, use of Federal Supply schedule contracts prior to these events to acquire products or services to be used to facilitate recovery is authorized. State or local governments will be responsible for ensuring that purchased products or services are to be used to facilitate recovery.

GSA provides additional information on the Disaster Recovery Purchasing Program website at <http://www.gsa.gov/disasterrecovery>.

State and local governments can find a list of eligible contractors on GSA's website, <http://www.gsa.elibrary.gsa.gov>, denoted with a  or  symbol.

Assistance is available from GSA on the Cooperative Purchasing and Disaster Purchasing Program at the local and national levels. For assistance at the local level, visit <http://www.gsa.gov> to find the point of contact in your area. For assistance at the national level, contact Tricia Reed at patricia.reed@gsa.gov, 571-259-9921. More information is available at <http://www.gsa.gov/cooperativepurchasing> and <http://www.gsa.gov/disasterrecovery>.

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

States and local jurisdictions to design, develop, conduct, and evaluate effective exercises.

In FY 2008, States may receive direct support for three exercises: one Training & Exercise Plan Workshop (T&EPW); one discussion-based exercise; and one operations-based exercise. While States are allowed to submit as many direct support applications as they choose, they are strongly encouraged to give careful thought to which exercises will require the additional assistance that will be provided through the direct support program. Exercises involving cross-border or mass-gathering issues will be counted against the number of direct-support exercises being provided to States.

Applications for direct support are available at <http://hseep.dhs.gov> and are reviewed on a monthly basis. The Homeland Security Exercise and Evaluation Program offers several tools and resources to help design, develop, conduct and evaluate exercises.

5. Homeland Security Preparedness Technical Assistance Program. The Homeland Security Preparedness Technical Assistance Program (HSPTAP) provides technical assistance on a first-come, first-served basis (and subject to the availability of funding) to eligible organizations to enhance their capacity and preparedness to respond to CBRNE terrorist incidents. In addition to the risk assessment assistance already being provided, FEMA also offers a variety of other technical assistance programs.

More information can be found at <http://www.fema.gov/government/grant/index.shtm>.

6. Lessons Learned Information Sharing (LLIS) System. LLIS is a national, online, secure website that houses a collection of peer-validated lessons learned, best practices, AARs from exercises and actual incidents, and other relevant homeland security documents. LLIS facilitates improved preparedness nationwide by providing response professionals with access to a wealth of validated front-line expertise on effective planning, training, equipping, and operational practices for homeland security.

The LLIS website also includes a national directory of responders and homeland security officials, as well as an updated list of homeland security exercises, events, and conferences. Additionally, LLIS includes online collaboration tools, including secure e-mail and message boards, where users can exchange information. LLIS uses strong encryption and active site monitoring to protect all information housed on the system. The LLIS website is <https://www.llis.gov>.

7. Information Sharing Systems. DHS encourages all State, regional, local, and Tribal entities using FRSGP funding in support of information sharing and intelligence fusion and analysis centers to leverage available Federal information sharing systems, including Law Enforcement Online (LEO) and the Homeland Security Information Network (HSIN). For additional information on LEO, contact the LEO Program Office at leoprogramoffice@leo.gov or (202) 324-8833. For additional information on HSIN and available technical assistance, contact the HSIN Help Desk at (703) 674-3003

Appendix K
Vulnerability Assessment and Security Plan
Certification Form to Apply for Railroad Frontline
Employee Training

Railroad carriers that have already completed a vulnerability assessment and developed and implemented a security plan that meet the requirements of Appendix E (Vulnerability Assessments) and Appendix F (Security Plans) can use this form as their certification, and submit it as part of their grant application. All railroad carriers that use this certification form must be able to provide both their existing vulnerability assessment and security plan upon request.

I, [insert name], as [insert title] of [insert name of freight railroad carrier], certify that a vulnerability assessment has been completed and a security plan has been developed and implemented. This vulnerability assessment includes all elements required as listed in Appendix E of the FY 2008 Freight Rail Security Grant Program Guidance and Application Kit. This security plan includes all elements required as listed in Appendix F of the FY 2008 Freight Rail Security Grant Program Guidance and Application Kit.

Signature

Date

Appendix L
Vulnerability Assessment and Security Plan
Certification Form for 49 CFR Part 172

Railroad carriers that have already completed a vulnerability assessment and developed and implemented a security plan in accordance with 49 CFR part 172 can use this form as their certification and submit it as part of their grant application. All railroad carriers that use this certification form must be able to provide both the vulnerability assessment and security plan upon request.

I, [insert name], as [insert title] of [insert name of freight railroad carrier], certify that a vulnerability assessment has been completed and a security plan has been developed and implemented. This vulnerability assessment and security plan is in compliance with 49 CFR part 172.

Signature

Date