



U.S. DEPARTMENT OF HOMELAND SECURITY

FISCAL YEAR 2010

FREIGHT RAIL SECURITY GRANT PROGRAM

GUIDANCE AND APPLICATION KIT

DECEMBER 2009



U.S. DEPARTMENT OF HOMELAND SECURITY

Title of Opportunity: FY 2010 Freight Rail Security Grant Program (FRSGP)

Funding Opportunity Number: DHS-10-GPD-075-000-01

Federal Agency Name: U.S. Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA)

Announcement Type: Initial

Dates: Completed applications must be submitted **no later than 11:59 p.m. EST, February 12, 2010.**

Additional overview information: The Fiscal Year (FY) 2010 Freight Rail Security Grant Program (FRSGP) contains significant improvements based on extensive outreach to grant participants and stakeholders. Some of the key changes impacting the FY 2010 FRSGP as compared to the previous year's program include the following:

Funding Priorities

The funding priorities include the following project types for the FY 2010 FRSGP:

- Global Positioning System (GPS) tracking
- Vulnerability Assessments and Security Plans
- Security training and exercises for railroad frontline employees
- Infrastructure hardening on rail bridges spanning the Western Rivers System

Cost Share Requirement

The FY 2010 FRSGP has a 75 percent Federal and 25 percent grantee cost share cash or in-kind match requirement. The non-federal contribution may be cash or in-kind as defined under 44 CFR 13.24. Vulnerability assessments and security plans are exempt from this cost share requirement.

Management and Administration

Management and Administration (M&A) may not exceed five percent (5%) of the total award for grantees.

Additional Considerations

- No minimum project cost requirement
- Funding release of project design/planning costs for eligible projects when identified clearly in the Investment Justification/Budget Detail Worksheet
- Revised scoring criteria for project approval

CONTENTS

Contents.....	1
Part I. FUNDING OPPORTUNITY DESCRIPTION.....	2
Part II. AWARD INFORMATION	13
Part III. ELIGIBILITY INFORMATION	14
A. Eligible Applicants.....	14
B. Cost Sharing	17
C. Restrictions	17
Part IV. APPLICATION AND SUBMISSION INFORMATION	18
A. Address to Request Application Package	18
B. Content and Form of Application	18
C. Submission Dates and Times	23
D. Intergovernmental Review	23
E. Funding Restrictions	23
F. Other Submission Requirements	26
Part V. APPLICATION REVIEW INFORMATION	27
A. Review Criteria.....	27
B. Review and Selection Process	28
C. Anticipated Announcement and Award Dates	28
Part VI. AWARD ADMINISTRATION INFORMATION	29
A. Notice of Award	29
B. Administrative and National Policy Requirements	29
C. Reporting Requirements	38
Part VII. FEMA CONTACTS.....	42
Part VIII. OTHER INFORMATION	45
A. Investment Justification Template	45
B. Sample Budget Detail Worksheet.....	50
C. Vulnerability Assessment and Security Plan Certification Statement	53
D. Owner and Offerors Concurrence Statement.....	54
E. Other	55

PART I.

FUNDING OPPORTUNITY DESCRIPTION

The Freight Rail Security Grant Program (FRSGP) is a 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) 2010 focus on transportation infrastructure security activities. These grant programs are part of 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 is an important component of the Department's effort to enhance the security of the Nation's critical infrastructure. The program provides funds to freight railroad carriers and owners and offerors of railroad cars to protect critical surface transportation infrastructure from acts of terrorism, major disasters, and other emergencies. The FY 2010 FRSGP is authorized by section 1406 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Public Law 110-53) (the 9/11 Act) and the *Department of Homeland Security Appropriations Act, 2010* (Public Law 111-83).

The funding priorities for the FY 2010 FRSGP reflect the Department's overall investment strategy. Of these priorities two have been paramount—risk-based funding and regional security cooperation. This document also reflects changes called for in the 9/11 Act.

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). 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.

The National Preparedness Guidelines define a vision of what to accomplish and provide 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. They outline 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 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. The 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. Additional information may also be found at <http://www.dhs.gov/xprepresp/publications>.

Funding Priorities

The funding priorities for the FY 2010 FRSGP reflect the Department's overall investment strategy as well as requirements of the 9/11 Act. The key goals of the FY 2010 FRSGP are to establish the basis for capital security improvements by funding vulnerability assessments and security plans, training to frontline personnel, security-related exercises, GPS tracking on railroad cars, and infrastructure hardening on rail bridges spanning the Western River System. Infrastructure hardening is defined as the act of applying security to the infrastructure including but not limited to; Access Control Systems, Video Monitoring Systems, and Physical Barriers. It does not include non-security related investments.

The Department, in alignment with the 9/11 Act, identifies the following specific priorities for the FY 2010 FRSGP as the **only allowable uses of funds** under this year's program. For more detail about what specific activities are allowable uses on funds please see Part IV.E., "Funding Restrictions".

- 1. GPS tracking.** Owners and offerors¹ of railroad cars used in the transportation of poisonous by inhalation/toxic inhalation hazardous (TIH) materials as defined in Part III. A of this FY 2010 guidance document may apply for funds to acquire, install, and operate satellite GPS tracking on those railroad cars for the period of performance. For purposes of this grant program, "offerors" are entities that lease rail cars in order to ship materials poisonous by inhalation/TIH materials by railroad.

While the Department realizes there may be other security-sensitive materials transported by rail, the vast majority of security-sensitive materials rail shipments are materials poisonous by inhalation/TIH materials; therefore, the GPS tracking program of this grant effort will focus on TIH shipments.

If security-sensitive materials offerors who ship by railroad apply for GPS tracking on cars that transport TIH, they must also submit a statement certifying the acknowledgment of the application by the owner of the rail car. A concurrence statement can be found in Part IV.B. "Content and Form Application" and must be submitted as part of the application submission. Both owners of railroad cars and offerors may not receive funding for the same rail car. If an eligible owner and an eligible offeror submit an application for the same rail car, priority will be given to the owner of the rail car. All eligible applicants must submit the numbers of the railcars on which they are planning to install GPS equipment.

¹ "Security-sensitive materials offerors who ship by railroad" are authorized as eligible applicants by the 9/11 Act.

Satellite tracking equipment must be able to meet specific communication protocol standards that are outlined in Part IV of this grant guidance document. Note that adherence to these components is one factor in grant application evaluation. The tracking information obtained using this GPS equipment will be owned by the railcar owner who will allow unrestricted access to DHS/Transportation Security Agency (TSA) as a condition of the award.

- 2. 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 mitigation strategies) will form the basis of funding priorities for this grant program in future years, as appropriate. For more information about the components of a vulnerability assessment and security plan to be completed with FY 2010 FRSGP funds, see pages 7-10. Note that adherence to these components is one factor in grant application evaluation.

Freight railroad carriers without comprehensive vulnerability assessments and security plans will not be considered for other projects.

Only Class II and Class III railroad carriers are eligible to apply for vulnerability assessment and security planning funds. 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. Eligible Class II and Class III freight 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 to meet the requirements listed in Part I. If the applicant's current vulnerability assessment and security plan comply fully with the requirements of the FY 2010 Freight Rail Security Grant Program Guidance and Application Kit, and **only** if the applicant certifies to that, then the applicant may apply to enhance its current vulnerability assessment and security plan, conduct security training for railroad frontline employees, and/or conduct security-related exercises. A certification form can be found in Part IV.B. "Content and Form Application" and must be submitted as part of the application submission.

- 3. Security training and exercises 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. For more information about the components of a training program to be completed with FY 2010 FRSGP funds, see pages 10-12.

Note that adherence to these components is one factor in grant application evaluation.

Security exercises, either in conjunction with training or separately, is allowable. The exercises must be focused on antiterrorism. Exercises that are regionally collaborative and included outside security partners are encouraged.

Please note that applicants for training and exercise funds will be required to certify the existence of both a vulnerability assessment and security plan that comply fully with the requirements of the FY 2010 Freight Rail Security Grant Program Guidance and Application Kit to be eligible for training under the FY 2010 FRSGP. A certification form can be found in Part VIII. "Other Information" and must be submitted as part of the application submission.

4. Infrastructure hardening on rail bridges spanning the Western Rivers System
Western Rivers System. Owners of rail bridges which span Western Rivers System and which are used for freight rail transportation may apply for infrastructure hardening capabilities. Additional information is available on page 12.

Eligible applicants are divided into four groups based on the types of projects they can apply for: Class I railroad carriers, Class II/III railroad carriers, owners and offerors of railroad cars that transport TIH by rail, and owners of railroad bridges spanning the Western Rivers System.

Eligible Class I railroad carriers may **only** request funding for security awareness and emergency response training for railroad frontline employees and security exercises. 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 listed in Part I.

Eligible Class II and Class III freight 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 to meet the stronger requirements that are listed in Part I. Upon completion of the vulnerability assessment and security plan that meets the stronger requirements listed in Part I, eligible Class II and Class III railroad carriers may request funding for security awareness and emergency response training for railroad frontline employees and security exercises. In order for these projects to be funded, the carrier must first certify that the requirements for vulnerability assessments and security plans, listed in Part I have been met. A certification form can be found in Part IV.B. "Content and Form Application" and must be submitted as part of the application submission. If these items have already been completed, an eligible applicant may request funds for security training and/or exercises.

Eligible owners and offerors of railroad cars may use grant funds received under this program to acquire, install, and operate satellite GPS tracking on cars that transport TIH

over the period of performance. Satellite tracking equipment must be able to meet specific communication protocol standards that are outlined in Part IV. The tracking information obtained using this GPS equipment will be owned by the railroad car owner who will allow unrestricted access to DHS/TSA as a condition of the award. In order to request FY 2010 FRSGP funds, applicants must complete and submit an Investment Justification, the outline of which is provided in Part VIII of the FY 2010 FRSGP grant guidance.

GPS Tracking Requirements

Bulk-TIH Rail Car Tracking Systems

Implement tracking of rail cars transporting bulk amounts of TIH materials throughout the United States using satellite and/or land-based wireless GPS communications systems. The tracking systems requirements shall include the following:

- The system shall have the capability of providing the current position by latitude and longitude.
- The system shall have geofencing capabilities that allow authorized users to define and monitor routes through High Threat Urban Areas (HTUAs).
- The system shall have the capability of sending an alert notification to the designated dispatch/operation center when the rail car enters and leaves an HTUA.
- The system shall have the capability to allow polling of the rail car tracking units to request a current location and status report.
- The system shall be capable of operating with a reporting frequency that permits locating the rail car within a reasonable precision when requested by DHS/TSA representatives.
- The tracking system shall meet all Federal, State, local, and industry safety standards regarding the installation of the GPS equipment on the rail car.

The tracking system shall be tested periodically and the results of the test recorded.

Technology Standards

Rail Car Tracking Systems shall conform to the “TSA Universal Communications Interface (UCI) – Interface Requirements Specification (IRS)” for enabling the transmission of data from commercially available tracking systems to a centralized government tracking center. The TSA UCI Interface Control Document provides the details to enable a commercial rail car tracking system to implement the nonproprietary universal interface set of protocols.

Data Requirements

The UCI provides the means for rail car owners and lessees to provide a government centralized tracking center with tracking data including information regarding Transportation Security Incidents involving rail cars transporting bulk amounts of TIH materials. Companies must provide TSA rail car tracking and shipment data through the UCI.

Communications Plan

A communications plan should be established to include standard operating procedures (SOP) for communications between rail car owners/lessees, appropriate railroad carrier personnel, and emergency services agencies. This plan should include the appropriate two-way communication technologies required to implement the communications plan, such as terrestrial or satellite-based systems. This is not intended to preclude the use of personal cell phones.

Please also read Part IV.E. for information on funding restrictions. Applicants should send an email to TSAGrants@tsa.dhs.gov for additional information.

Vulnerability Assessment Requirements

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 security-sensitive materials (SSM) in rail cars, excluding residue.

Vulnerability Assessment Structure

A rail carrier vulnerability assessment shall include:

- 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.
- Each asset should be assessed as the target of at least the following acts of terrorism (attack scenarios): a vehicle born improvised explosion device (VBIED) attack, an improvised explosion device (IED) attack, and a cyber attack (if applicable). Additional attack scenarios should be assessed if applicable.
- 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:
 - Physical security including fencing, alarms, monitoring using cameras and patrols, warning signs, and lighting;
 - Randomness of operations;
 - Access control of employees, contractors, visitors, and trespassers to critical areas;
 - Programmable electronic devices, computers, or other automated systems which are used in providing the transportation;
 - Communications systems and utilities needed for railroad security purposes including dispatching and notification systems;
 - Planning including the coordination with the public emergency responders and law enforcement agencies;
 - Employee and contractor personnel screening;
 - Employee security training, and;

- Dwell time of rail cars containing SSM cars in rail yards, terminals, and on railroad-controlled leased track.
- 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.
- 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.
- 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.

Vulnerability Assessment Methodologies

The rail carrier vulnerability assessment must be conducted using a tool or methods which meet 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.

Please also read Part IV.E. for information on funding restrictions.

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

Security Plan Requirements

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.

Freight Rail Security Plan Structure

The Plan should address the following elements, as applicable:

- Rail Carrier's Statement of Security Plan Objectives (what the plan sets out to do)
- 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
- Roles and responsibilities of those designated with security responsibilities.
- Procedures in place to communicate, disseminate, and respond to threat information
- 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)

- Security countermeasures to be implemented by your railroad in response to a terrorist attack or threat incident at each alert level (blue to red)
- Procedures in place for periodic audits, exercises and drills for security plans and for its amendment in response to experience
- Measures to prevent unauthorized access to designated or restricted areas
- Measures to prevent the introduction of dangerous substances and devices to designated restricted areas and/or railroad property
- 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
- Identifications of security processes to work with State and local law enforcement agencies, emergency responders, and Federal officials in response to a terrorist attack
- Procedures for evacuating railroad facilities or conveyances in case of reliable security threats or breaches of security
- Procedures in place for protection of railroad carrier designated critical infrastructures
- Procedures for employee identification and background checks for employees and contractors
- 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, and crisis management organizational representatives in local areas, including 24 hour contact details
- 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 by contractual agreements
- Procedures to address secure handling and storage of toxic inhalation hazardous materials when threat conditions warrant
- Plans to minimize the occasions when loaded tank cars carrying TIH materials are unattended in HTUAs
- Plan for employee security awareness training to include timeline for conducting employee training
- Plans for a positive and secure handoff of SSM rail cars at points of interchange with shippers, receivers, and other carriers
- Plans and procedures to provide redundant and backup systems required to ensure continued railroad operations
- Procedures to respond to and facilitate the recovery of the railroad operations after a transportation security incident
- Procedures for cyber security

- Appendix containing risk mitigation strategies for addressing vulnerabilities identified in the vulnerability assessment but not sufficiently addressed by the security plan. This should include:
 - Outstanding vulnerabilities
 - Mitigation options and associated costs of alternatives
 - Preferred mitigation strategy
 - Comprehensive funding plan and schedule for risk remediation

Please also read Part IV.E. for information on funding restrictions.

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

Frontline Employee Security Training Program Requirements

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;
 - c. Recognizing the characteristics of IED and weapons of mass destruction (WMD) and reporting and reacting to these threats in the confines of trains and critical infrastructure;
 - d. Identifying and maintaining domain awareness of Rail Security Sensitive Material (RSSM) shipments and associated manifest paperwork; and
 - e. Understanding RSSM Chain of Custody Requirements.
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, detection, deterrence and response activities for threats or incidents involving IEDs, VBIEDs, and WMD;
 - c. Understanding individual roles and responsibilities in prevention of, protection against, detection of, deterrence of, 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, detection of, deterrence of and response to a terrorist threat or attack;
 - e. Directing and coordinating prevention, protection detection, deterrence 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.

Requests for 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.

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 the subject areas described above.

The vendors providing training do not necessarily need to be DHS-approved vendors. If 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. Please also read Part IV.E, for information on funding restrictions. Applicants should send an email to TSAGrants@tsa.dhs.gov for additional information.

Infrastructure Hardening on Rail Bridges spanning the Western Rivers System Requirements

To be eligible for infrastructure hardening funding, bridges must have a volume exceeding 4.9 million gross ton miles (MGTM) and span a waterway considered part of the Western Rivers System.

Applicants must include a monitoring plan describing how security capabilities will be continuously monitored with a 24/7 commitment. Infrastructure hardening is limited to the bridge structure and immediate surrounding area and access points.

Bridges that have already received Federal funding for infrastructure hardening are ineligible for additional funds through the FY 2010 FRSGP.

Please also read Part IV.E for information on funding restrictions. Applicants should send an email to TSAGrants@tsa.dhs.gov for additional information.

FRSGP Program Management: Roles and Responsibilities at DHS

Effective management of the FRSGP entails a collaborative effort and partnership within DHS, the dynamics of which require continuing outreach, coordination and interface. For the FY 2010 FRSGP, FEMA is responsible for designing and operating the administrative mechanisms needed to implement and manage the grant program. TSA provides programmatic subject matter expertise for the transportation industry and assists by coordinating the myriad of intelligence information and risk/vulnerability assessments resulting in ranking and rating rail and mass transit assets nationwide against threats associated with potential terrorist attacks and in defining the parameters for identifying, protecting, deterring, responding, and recovering from such incidents. Together, these two agencies with additional assistance and cooperation of the Federal Transit Administration (FTA), for rail and mass transit systems, and the Federal Railroad Administration (FRA), as needed for freight rail operations, determine the primary security architecture of the FRSGP.

PART II.

AWARD INFORMATION

Authorizing Statutes

Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53) (6 U.S.C. §1135 et seq.) and the Homeland Security Act of 2002 (6 U.S.C. §101 et seq.) and the Department of Homeland Security Appropriations Act, 2010 (Public Law 111-83).

Period of Performance

The period of performance of this grant is 36 months. Extensions to the period of performance will be considered only through formal requests to FEMA with specific and compelling justifications as to why an extension is required.

Available Funding

In FY 2010, the total amount of funds distributed under this grant will be \$15,000,000.

PART III.

ELIGIBILITY INFORMATION

A. Eligible Applicants

Eligible applicants for the FY 2010 FRSGP are determined by DHS as Class I, II, and III freight railroad carriers that transport RSSM as defined in 49 CFR Part 1580.100 B and owners and offerors of railroad cars that transport TIH materials as defined in 49 CFR 171.8. For purposes of this grant program, “offerors” are entities that lease rail cars in order to ship materials poisonous by inhalation/TIH materials by railroad.

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.

Class I, II, and III freight railroad carriers must also meet the following criteria in order to be eligible:

- Transport RSSM. RSSM is defined in 49 CFR Part 1580.100 B as: (1) A rail car containing more than 2,268 kg (5,000 lbs) of a Division 1.1, 1.2, or 1.3 (explosive) material, as defined in 49 CFR 173.50; (2) A tank car containing a material poisonous by inhalation as defined in 49 CFR 171.8, including anhydrous ammonia, Division 2.3 gases poisonous by inhalation as set forth in 49 CFR 173.115(c), and Division 6.1 liquids meeting the defining criteria in 49 CFR 173.132(a)(1)(iii) and assigned to hazard zone A or hazard zone B in accordance with 49 CFR 173.133(a), excluding residue quantities of these materials; and (3) A rail car containing a highway route-controlled quantity of a Class 7 (radioactive) material, as defined in 49 CFR 173.403.
- Operate in or through a HTUA, as subject to the forthcoming “Rail Transportation Security Final Rule,” and as identified in Table 1 of the FY 2010 Freight Rail Security Grant Program Guidance and Application Kit.
- Certify they have developed and adhere to a vulnerability assessment and security plan that conforms to the requirements of 49 CFR 172.802².

² 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.”

**Table 1:
FY 2010 FREIGHT RAIL SECURITY HIGH THREAT URBAN AREAS (HTUA)**

FY 2010 Tier I Urban Areas			
State/Territory	Urban Area	State/Territory	Urban Area
California	Bay Area	New Jersey	Jersey City/Newark Area
	Los Angeles/Long Beach Area	New York	New York City Area
District of Columbia	National Capital Region	Pennsylvania	Philadelphia Area
Illinois	Chicago Area	Texas	Dallas/Fort Worth/Arlington Area
Massachusetts	Boston Area		Houston Area
FY 2010 Tier II Urban Areas			
State/Territory	Urban Area	State/Territory	Urban Area
Arizona	Phoenix Area	Nebraska	Omaha Area
	Tucson Area	Nevada	Las Vegas Area
California	Anaheim/Santa Ana Area	New York	Albany Area
	Bakersfield Area		Buffalo Area
	Oxnard Area		Rochester Area
	Riverside Area		Syracuse Area
	Sacramento Area	North Carolina	Charlotte Area
	San Diego Area	Ohio	Cincinnati Area
Colorado	Denver Area		Cleveland Area
Connecticut	Bridgeport Area		Columbus Area
	Hartford Area		Toledo Area
Florida	Fort Lauderdale Area	Oklahoma	Oklahoma City Area
	Jacksonville Area		Tulsa Area
	Miami Area	Oregon	Portland Area
	Orlando Area	Pennsylvania	Pittsburgh Area
	Tampa Area	Puerto Rico	San Juan Area
Georgia	Atlanta Area	Rhode Island	Providence Area
Hawaii	Honolulu Area	Tennessee	Memphis Area
Indiana	Indianapolis Area		Nashville Area
Kentucky	Louisville Area	Texas	Austin Area
Louisiana	Baton Rouge Area		El Paso Area
	New Orleans Area		San Antonio Area
Maryland	Baltimore Area	Utah	Salt Lake City Area
Michigan	Detroit Area	Virginia	Norfolk Area
Minnesota	Twin Cities Area		Richmond Area
Missouri	Kansas City Area	Washington	Seattle Area
	St. Louis Area	Wisconsin	Milwaukee Area

Freight railroad carriers may apply for training and exercises if they **certify they have completed a vulnerability assessment and security plan that meet the requirements outlined in Part I.** This grant program does not cover the expenses

associated with conducting a vulnerability assessment or developing a security plan for Class I freight railroad carriers.

Eligible Class II and Class III freight 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 to meet the requirements. Funds may also be used to improve upon an existing security plan to meet the requirements. Eligible Class II and Class III freight railroad carriers may request funding for security awareness and emergency response training for railroad frontline employees, and/or security exercises only if they can certify that the requirements for vulnerability assessments and security plans listed in Part I have been met by their existing vulnerability assessment and implemented security plan.

Owners and offerors of railroad cars must meet the following criteria in order to be eligible:

- Transport Rail TIH. For the purpose of this grant, TIH is defined as: 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.
- Travel from, to or through a HTUA.

Please refer to Part VIII for examples of certification statements. These statements must be submitted as part of the grant application, as applicable.

National Incident Management System (NIMS) Implementation Compliance

In accordance with Homeland Security Presidential Directive (HSPD)-5, *Management of Domestic Incidents*, the adoption of the NIMS is a requirement to receive Federal preparedness assistance, through grants, contracts, and other activities. The NIMS provides a consistent nationwide template to enable all levels of government, tribal nations, nongovernmental organizations, and private sector partners to work together to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity.

Federal FY 2009 NIMS implementation must be considered prior to allocation of any Federal preparedness awards in FY 2010. In April 2009, the National Integration Center Incident Management Systems Integration (IMSI) Division advised State, tribal nation, and local governments to respond to metric assessments in the NIMS Compliance Assistance Support Tool (NIMSCAST) to assess on-going progress and achievement.³ The list of objectives against which progress and achievement are assessed and reported can be found at

<http://www.fema.gov/emergency/nims/ImplementationGuidanceStakeholders.shtm#item2>.

³ As defined in the *Homeland Security Act of 2002* (Public Law 107-296), the term "State" means "any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States" 6 U.S.C. 101 (14).

All State, tribal nation, and local government grantees were required to update their respective NIMSCAST assessments by September 30, 2009. State, tribal, and local grantees unable to meet implementation objectives were required to submit a Corrective Action Plan via NIMSCAST no later than October 31, 2009. Comprehensive information concerning NIMS implementation for States, tribal nations, local governments, nongovernmental organizations, and the private sector is available through IMSI via its NIMS Resource Center at www.fema.gov/nims.

States, tribal nations, and local governments should continue to implement the training guidance contained in the *Five-Year NIMS Training Plan*, released in February 2008.

The primary grantee/administrator of FY 2010 FRSGP award funds is responsible for determining if sub-awardees have demonstrated sufficient progress to disburse awards.

B. Cost Sharing

The FY 2010 FRSGP has a 75 percent Federal and 25 percent grantee cost share cash- or in-kind match requirement. The non-federal contribution may be cash or in-kind as defined under 44 CFR 13.24. Vulnerability assessments and security plans are exempt from this cost share requirement.

C. Restrictions

Please see Part IV.E. for Management and Administration (M&A) limits, and allowable/unallowable costs guidance.

Part IV.
**APPLICATION AND SUBMISSION
INFORMATION**

A. Address to Request Application Package

All applications for DHS grants will be filed using the common electronic “storefront” – www.grants.gov. To access application forms and instructions, select “Apply for Grants,” and then select “Download Application Package.” Enter the Catalog of Federal Domestic Assistance (CFDA) and/or the funding opportunity number located on the cover of this announcement. Select “Download Application Package,” and then follow the prompts to download the application package. To download the instructions, go to “Download Application Package” and select “Instructions.” If you experience difficulties or have any questions, please call the www.grants.gov customer support hotline at (800) 518-4726.

DHS may request original signatures on forms at a later date.

B. Content and Form of Application

The on-line application must be completed and submitted using www.grants.gov after Central Contractor Registry (CCR) registration is confirmed. The on-line application includes the following required forms and submissions:

- Investment Justification
- Budget Detail Worksheet
- Standard Form 424, Application for Federal Assistance
- Standard Form 424A, Budget Information
- Standard Form 424B, Assurances
- Standard Form 424C, Budget Information – Construction Form
- Standard Form 424D, Assurances – Construction Programs
- Lobbying Form – Certification Regarding Lobbying (this form must be completed by all grant applicants)
- Standard Form LLL, Disclosure of Lobbying Activities (if the grantee has engaged or intends to engage in lobbying activities)
- Certification Regarding Debarment, Suspension, and Other Responsibility Matters
- Certification Regarding Drug Free Workplace Requirements

The program title listed in the CFDA is “*Rail and Transit Security Grant Program.*” The CFDA number is **97.075**.

1. **Application via www.grants.gov.** All applicants must file their applications using the Administration's common electronic "storefront" - www.grants.gov. Eligible grantees must apply for funding through this portal, accessible on the Internet at www.grants.gov.
2. **Dun and Bradstreet Data Universal Numbering System (DUNS) number.** The applicant must provide a DUNS number with their application. This number is a required field within www.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 (866) 705-5711.
3. **Valid 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 www.grants.gov.
4. **Investment Justification.** As part of the FY 2010 FRSGP application process, applicants must develop a formal Investment Justification that addresses each initiative being proposed for funding. These Investment Justifications must demonstrate how proposed projects address gaps and deficiencies in current programs and capabilities. The Investment Justification must demonstrate the ability to provide enhancements consistent with the purpose of the program and guidance provided by FEMA. Applicants must ensure that the Investment Justification is consistent with all applicable requirements outlined in this application kit.

Applicants may propose up to four investments within their application. A separate Investment Justification must be submitted for each proposed project. All Investment Justifications must be submitted with the application by February 12, 2010.

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 www.grants.gov, no later than 11:59 p.m. EST, February 12, 2010. Applicants must submit one SF-424, as well as an Investment Justification and detailed budget for each project.

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

- I. Background;
- II. Impact;
- III. Implementation Plan.

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

Investment Justification Submission and File Naming Convention

Investment Justifications must be submitted with the grant application as a file attachment within www.grants.gov. Applicants must use the following file naming convention when submitting Investment Justifications as part of the FY 2010 FRSGP:

Investment Justification (through www.grants.gov file attachment)

Company Name_IJ Number (Example: ABC Railroad_IJ#1)

Applicants will find a sample Investment Justification worksheet in Part VIII. This worksheet may be used as a guide to assist applicants in the preparation of the Investment Justification.

Detailed Budget Submission and File Naming Convention

Investment Justifications must be submitted with the grant application as a file attachment within www.grants.gov. Applicants must use the following file naming convention when submitting detailed budgets as part of the FY 2010 FRSGP:

Detailed Budget (through www.grants.gov file attachment)

Company Name_IJ Number_Budget (Example: ABC Railroad_IJ#1_Budget)

Applicants will find a sample Budget Detail Worksheet in Part VIII. This worksheet may be used as a guide to assist applicants in the preparation of the budget and budget narrative.

- 5. Vulnerability Assessment.** 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 (See Part VIII. "Other Information" for the Vulnerability and Assessment Certification Statement).

Vulnerability Assessment Structure

A rail carrier Vulnerability Assessment shall include:

- 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.
- 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.
- 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:
 - Physical security including fencing, alarms, monitoring using cameras and patrols, warning signs and lighting;

- Randomness of operations;
- Access control of employees, contractors, visitors and trespassers to critical areas;
- Programmable electronic devices, computers, or other automated systems which are used in providing the transportation;
- Communications systems and utilities needed for railroad security purposes including dispatching and notification systems;
- Planning including the coordination with the public emergency responders and law enforcement agencies;
- Employee and contractor personnel screening;
- Employee security training, and;
- Dwell time of rail cars containing SSM cars in rail yards, terminals, and on railroad-controlled leased track.
- 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.
- 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.
- 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 success of the act of terrorism and threat information available to the rail carrier.

Vulnerability Assessment Methodologies

The rail carrier vulnerability assessment must be conducted using a tool or methods which meet 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 TRAM and the Intelligence Community's ARM Process. Various commercially available tools meet these criteria.

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

6. **Security Plan.** 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 (See Part VIII. "Other Information" for the Vulnerability and Assessment Certification Statement).

Freight Rail Security Plan Structure

The Plan should address the following elements, as applicable:

- Rail Carrier's Statement of Security Plan Objectives (what the plan sets out to do)

- 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
- Roles and responsibilities of those designated with security responsibilities
- Procedures in place to communicate, disseminate, and respond to threat information
- 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)
- Security countermeasures to be implemented by your railroad in response to a terrorist attack or threat incident at each alert level (blue to red)
- Procedures in place for periodic audits, exercises and drills for security plans, and for its amendment in response to experience
- Measures to prevent unauthorized access to designated or restricted areas.
- Measures to prevent the introduction of dangerous substances and devices to designated restricted areas and/or railroad property
- 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
- Identifications of security processes to work with State and local law enforcement agencies, emergency responders, and Federal officials in response to a terrorist attack
- Procedures for evacuating railroad facilities or conveyances in case of reliable security threats or breaches of security
- Procedures in place for protection of railroad carrier designated critical infrastructures
- Procedures for employee identification and background checks for employees and contractors
- 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
- 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 by contractual agreements
- Procedures to address secure handling and storage of toxic inhalation hazardous materials when threat conditions warrant
- Plans to minimize the occasions when loaded tank cars carrying TIH materials are unattended in HTUAs
- Plan for employee security awareness training to include timeline for conducting employee training
- Plans for a positive and secure handoff of SSM rail cars at points of interchange with shippers, receivers and other carriers

- Plans and procedures to provide redundant and backup systems required to ensure continued railroad operations
- Procedures to respond to and facilitate the recovery of the railroad operations after a transportation security incident
- Procedures for cyber security
- Appendix containing risk mitigation strategies for addressing vulnerabilities identified in the vulnerability assessment but not sufficiently addressed by the security plan. This should include:
 - Outstanding vulnerabilities
 - Mitigation options and associated costs of alternatives
 - Preferred mitigation strategy
 - Comprehensive funding plan and schedule for risk remediation

7. Owner and Offerors Concurrence Statement. Security sensitive materials offerors who ship by railroad and owners of railroad cars used in the transportation of security-sensitive materials may use grant funds received under this program to acquire and install satellite GPS tracking on rail cars that transport poisonous-by-inhalation/toxic inhalation hazardous (TIH) materials as defined in Part III.A. of the FY 2010 FRSGP guidance. Offerors applying for FY 2010 grant funding for GPS tracking can use the statement in Part VIII. “Other Information” to certify that the owner of the rail car acknowledges the grant application for the procurement of GPS tracking to attach to their rail car.

C. Submission Dates and Times

Application submissions will be received by **11:59 p.m. EST, February 12, 2010**. Only applications made through www.grants.gov will be accepted.

D. Intergovernmental Review

Executive Order 12372 requires applicants from State and local units of government or other organizations providing services within a State to submit a copy of the application to the State Single Point of Contact (SPOC), if one exists, and if this program has been selected for review by the State. Applicants must contact their State SPOC to determine if the program has been selected for State review. Executive Order 12372 can be referenced at <http://www.archives.gov/federal-register/codification/executive-order/12372.html>. The names and addresses of the SPOCs are listed on OMB’s home page available at <http://www.whitehouse.gov/omb/grants/spoc.html>.

E. Funding Restrictions

DHS grant funds may only be used for the purpose set forth in the grant, and must be consistent with the statutory authority for the award. Grant funds may not be used for matching funds for other Federal grants/cooperative agreements, lobbying, or intervention in Federal regulatory or adjudicatory proceedings. In addition, Federal funds may not be used to sue the Federal government or any other government entity.

Pre-award costs are allowable only with the written consent of DHS and if they are included in the award agreement.

Any M&A costs associated with individual projects submitted for consideration under the FY 2010 FRSGP must be included in the budget for that project and explicitly identified, in Category G “Other Costs”. M&A costs may not exceed five percent (5%) of the funds awarded for each individual project.

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

1. GPS tracking on railroad cars
2. Vulnerability Assessments and Security Plans
3. Training and Exercises
4. Equipment for bridge hardening
5. Management and Administration

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.

The following provides additional detail about each of these allowable expense categories, and identifies several specific unallowable costs:

1. GPS Tracking.

- **Purchase of new units.** Basic GPS unit capable of reporting requirements as specified in GPS Tracking requirements Part I. Additional sensory capability costs are not eligible and, if included, must be assumed by the railroad car owner. **This grant will not fund replacement units or more than one unit per railcar.**
- **Installation.** Applicable installation costs for the GPS units are allowable
- **Activity Feeds.** In accordance with the satellite Communication system and functional requirements as specified in the GPS Tracking Requirements Part I. Cost of additional sensory information is not eligible and, if included, must be assumed by the railroad car owner.

2. Development of Vulnerability Assessments and Security Plans. FY 2010 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 Part I., are allowable expenses.
- **Security Plans.** Development of all required content, as specified in Part I., are allowable expenses.

3. Training and Exercise Costs. FY 2010 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 complies with the requirements in Part I of the FY 2010 FRSGP Grant Guidance and Application Kit.

These costs must be in accordance with the Federal Acquisition Regulation (FAR) Part 31.2:

- **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 and exercise-related activities.
- **Public Sector Employee Overtime and Backfill Costs.** The entire amount of overtime costs, including payments related to backfilling personnel, which are the direct result of attendance at FEMA and/or approved training courses and programs or time spent on the design, development and conduct of exercises are allowable. These costs are allowed only to the extent the payment for such services is in accordance with the policies of the State or unit(s) of local government and has the approval of the State or the awarding agency, whichever is applicable. In no case is dual compensation allowable. That is, an employee of a unit of government may not receive compensation from their unit or agency of government AND from an award for a single period of time (e.g., 1:00 p.m. to 5:00 p.m.), even though such work may benefit both activities. Overtime and backfill of private sector employees are not eligible.
- **Travel.** Travel costs (i.e., airfare, mileage, per diem, hotel, etc.) are allowable as expenses by employees who are on travel status for official business related to the planning and conduct of the training and/or exercise project(s) or for attending DHS-approved courses. These costs must be in accordance with State law as highlighted in FAR Part 31.2. Recipients must also follow State regulations regarding travel. If a grantee does not have a travel policy they must follow Federal guidelines and rates, as explained in 2 CFR Part 215. Private sector employee travel costs are not allowable.
- **Exercise Planning Workshop.** Grant funds may be used to plan and conduct exercise planning workshop, to include costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, travel and exercise plan development.
- **Supplies.** Supplies are items that are expended or consumed during the course of the planning and conduct of the training and/or exercise project(s) (e.g., copying paper, gloves, tape, non-sterile masks, and disposable protective equipment).
- **Other Items.** These costs may include the rental of space/locations for planning and conducting training and exercises, exercise signs, badges, and similar materials.

4. Equipment for Bridge Hardening

- **Purchase of New Hardware.** Security hardening equipment, such as cameras, sensors, access control units and lighting are allowable
- **Installation.** Applicable installation costs for the equipment is allowable

5. M&A costs. FY 2010 FRSGP funds may be used for the following M&A costs and is limited to five percent (5%) of the total grant award:

- Hiring of full-time or part-time staff or contractors/consultants to assist with the management of the FY 2010 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 FAR Part 31.2.)
- Acquisition of authorized office equipment, including personal computers or laptops

Specific unallowable costs include:

- Expenditures for items such as general-use software (e.g., 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)
- Contingency Fees
- 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

F. Other Submission Requirements

Federal employees are prohibited from serving in any capacity (paid or unpaid) on any proposal submitted under this program. Federal employees may not receive funds under this award.

PART V.

APPLICATION REVIEW INFORMATION

A. Review Criteria

In order to be considered for funding by the National Review Panel, a complete application must be submitted. Applications that are incomplete will not be considered for funding. See Part IV.B, for a list of all required submission documents.

The following factors will be considered by a National Review Panel of subject matter experts in the evaluation of each of the Investment Justifications and detailed budgets. It is recommended that these factors be clearly demonstrated in the content of the application.

Having met all administrative and submission requirements (including certification and concurrence statements, as applicable), applications will be evaluated and ranked based on:

1. **Compliance – 20%.** Projects will be evaluated based on their adherence to the project type requirements listed in Part I of the guidance (e.g. vulnerability assessment requirements, security plan requirements, frontline employee training requirement, and GPS requirements)
2. **Cost Appropriateness – 20%.** Projects will be evaluated and prioritized based on the cost appropriateness of the project. The project cost levels should be commensurate with the security impact, and the proposed solution should be reasonable and advantageous over other possible solutions.
3. **Feasibility – 20%.** Projects will be evaluated based on the ability of the applicant to complete the proposed project within the proposed timeframes, the level of expertise and appropriateness of the management team as proposed, and the ability for the applicant to meet the challenges associated with the implementation of the project.
4. **Sustainability – 10%.** Projects will be evaluated and prioritized based on the ability of the applicant to sustain (e.g. maintain intended benefit) the investment after Federal grant funding has been expended.
5. **Risk – 30%.** DHS is committed to focusing the bulk of available funds on high-risk areas. As such, the risk associated with (1) HUTAs and (2) the type and amount of SSM including TIH materials hauled or stored will also be considered in the funding of the project.

During the application period, and in conjunction with industry associations, DHS will identify multiple opportunities for open dialogue between the Department and potential applicants, such as weekly conference calls and workshops. This commitment is intended to ensure a common understanding of the funding priorities and administrative requirements associated with the FY 2010 FRGSP, and to help in submission of projects that will have the highest impact on reducing risks for freight railroad companies and their customers.

B. Review and Selection Process

The FY 2010 FRSGP will use risk-based prioritization consistent with DHS policy outlined in the FRSGP Program Guidance and Application Kit. Applications will be reviewed and scored by a National Review Panel based on the review criteria outlined on the previous page. All applicants must comply with all administrative requirements -- including Investment Justifications, budgets, required forms and certifications, and application process requirements.

C. Anticipated Announcement and Award Dates

FEMA will evaluate and act on applications within 60 days following close of the application period, consistent with the *Department of Homeland Security Appropriations Act, 2010* (Public Law 111-83). Awards will be made on or before September 30, 2010.

PART VI.

AWARD ADMINISTRATION INFORMATION

A. Notice of Award

Upon approval of an application, the grant will be awarded to the grant recipient. The date that this is done is the “award date.” Notification of award approval is made through the Grants Management System (GMS). Once an award has been approved, a notice is sent to the authorized grantee official. Follow the directions in the notification to accept your award documents. The authorized grantee official should carefully read the award and special condition documents. If you do not receive a notification, please contact your FEMA Program Analyst for your award number. Once you have the award number, contact the GMS Help Desk at (888) 549-9901, option three, to obtain the username and password associated with the new award.

The period of performance is 36 months and begins on the Project Period/Budget Period start date listed in the award package. Any unobligated funds will be de-obligated at the end of the close-out 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. All extension requests must be submitted to FEMA at least 60 days prior to the expiration of the grant period of performance. The justification must address:

- Reason for delay;
- Current status of the activity/activities;
- Approved period of performance termination date and new project completion date;
- Remaining available funds, both Federal and non-Federal;
- Budget outlining how remaining Federal and non-Federal funds will be expended;
- Plan for completion including milestones and timeframe for achieving each milestone and the position/person responsible for implementing the plan for completion; and
- Certification that the activity/activities will be completed within the extended period of performance without any modification to the original Statement of Work approved by FEMA.

B. Administrative and National Policy Requirements

The recipient and any sub-recipient(s) must, in addition to the assurances made as part of the application, comply and require each of its subcontractors employed in the completion of the project to comply with all applicable statutes, regulations, executive orders, OMB circulars, terms and conditions of the award, and the approved application.

1. Standard Financial Requirements. The grantee and any subgrantee(s) shall comply with all applicable laws and regulations. A non-exclusive list of regulations commonly applicable to DHS grants are listed below:

1.1 – Administrative Requirements.

- 44 CFR Part 13, *Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments*
- 2 CFR Part 215, *Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations* (formerly OMB Circular A-110)

1.2 – Cost Principles.

- 2 CFR Part 225, *Cost Principles for State, Local, and Indian tribal Governments* (formerly OMB Circular A-87)
- 2 CFR Part 220, *Cost Principles for Educational Institutions* (formerly OMB Circular A-21)
- 2 CFR Part 230, *Cost Principles for Non-Profit Organizations* (formerly OMB Circular A-122)
- Federal Acquisition Regulations (FAR), Part 31.2 *Contract Cost Principles and Procedures, Contracts with Commercial Organizations*

1.3 – Audit Requirements.

- OMB Circular A-133, *Audits of States, Local Governments, and Non-Profit Organizations*

1.4 – Duplication of Benefits. There may not be a duplication of any Federal assistance, per 2 CFR Part 225, Basic Guidelines Section C.3 (c), which states: Any cost allocable to a particular Federal award or cost objective under the principles provided for in this Authority may not be charged to other Federal awards to overcome fund deficiencies, to avoid restrictions imposed by law or terms of the Federal awards, or for other reasons. However, this prohibition would not preclude governmental units from shifting costs that are allowable under two or more awards in accordance with existing program agreements. Non-governmental entities are also subject to this prohibition per 2 CFR Parts 220 and 230 and FAR Part 31.2.

2. Payment. DHS/FEMA uses the Direct Deposit/Electronic Funds Transfer (DD/EFT) method of payment to Recipients. To enroll in the DD/EFT, the Recipient must complete a Standard Form 1199A, Direct Deposit Form.

FEMA uses the FEMA Payment and Reporting System (PARS) for payments made under this program, <https://isource.fema.gov/sf269/> (Note: link connects to Federal Financial Report [SF-425]).

2.1 – Advance Payment. In accordance with Treasury regulations at 31 CFR Part 205, the Recipient shall maintain procedures to minimize the time elapsing between the transfer of funds and the disbursement of said funds (see 44 CFR Part 13.21(c)) regarding payment of interest earned on advances. In order to

request an advance, the Recipient must maintain or demonstrate the willingness and ability to maintain procedures to minimize the time elapsing between the transfer of funds from DHS and expenditure and disbursement by the Recipient. When these requirements are not met, the Recipient will be required to be on a reimbursement for costs incurred method.

2.2 – Forms. In order to download the Standard Form 1199A, the Recipient may use the following Internet site: <http://www.fms.treas.gov/ef/1199a.pdf>.

NOTE: FUNDS WILL NOT BE AUTOMATICALLY TRANSFERRED UPON ISSUANCE OF THE GRANT. GRANTEES MUST SUBMIT A REQUEST FOR ADVANCE/REIMBURSEMENT IN ORDER FOR THE FUNDS TO BE TRANSFERRED TO THE GRANTEE'S ACCOUNT.

3. Non-supplanting Requirement. 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.

4. Technology Requirements.

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

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

4.3 – 28 CFR Part 23 Guidance. FEMA requires that any information technology system funded or supported by these funds comply with 28 CFR Part 23, *Criminal Intelligence Systems Operating Policies*, if this regulation is determined to be applicable.

4.4 – Best Practices for Government Use of Closed Circuit Television (CCTV). DHS recommends that grantees seeking funds to purchase and install CCTV systems, or funds to provide support for operational CCTV systems, review and utilize the guidance in *Best Practices for Government Use of CCTV: Implementing the Fair Information Practice Principles* available on the DHS Privacy Office website at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf.

5. Administrative Requirements.

5.1 – Freedom of Information Act (FOIA). FEMA 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 FEMA 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 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.

5.2 – Protected Critical Infrastructure Information (PCII). The PCII Program, established pursuant to the *Critical Infrastructure Act of 2002* (Public Law 107-296) (CII Act), created a framework which enables members of the private sector, States, local jurisdictions, and tribal nations to voluntarily submit sensitive information regarding critical infrastructure to DHS. The Act provides statutory protection from public disclosure and civil litigation for CII that is validated as PCII. When validated as PCII, the information can only be shared with government employees who complete the training requirement, who have homeland security duties, and a need to know.

PCII accreditation is a formal recognition that the covered government entity has the capacity and capability to receive and store PCII appropriately. DHS encourages all States, local jurisdictions, and tribal nations to pursue PCII accreditation to cover their government agencies. Accreditation activities include signing a memorandum of agreement (MOA) with DHS, appointing a PCII Officer and developing a standard operating procedure for handling PCII. For additional information about PCII or the accreditation process, please contact the DHS PCII Program Office at pcii-info@dhs.gov.

5.3 – 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. – Provides that no person on the grounds of race, color, or national origin 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. Title VI also extends protection to persons with Limited English Proficiency (LEP). (42 U.S.C. §2000d et seq.)

- *Title IX of the Education Amendments of 1972*, as amended, 20 U.S.C. §1681 et. seq. – Provides that no person, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subject to discrimination under any education program or activity receiving Federal financial assistance.
- *Section 504 of the Rehabilitation Act of 1973*, as amended, 29 U.S.C. §794 – Provides that no otherwise qualified individual with a disability in the United States, shall, solely by reason of his or her disability, be excluded from the participation in, be denied the benefits of, or subject to discrimination in any program or activity receiving Federal financial assistance.
- *The Age Discrimination Act of 1975*, as amended, 20 U.S.C. §6101 et. seq. – Provides that no person in the United States shall, on the basis of age, be excluded from participation in, be denied the benefits of, or be subject 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.

5.4 – Services to Limited English Proficient (LEP) persons. Recipients of FEMA 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 proposals and budgets and in conducting their programs and activities. Reasonable costs associated with providing meaningful access for LEP individuals are considered allowable program costs. For additional information, see <http://www.lep.gov>.

5.5 – Certifications and Assurances. Certifications and assurances regarding the following apply:

- *Lobbying.* 31 U.S.C. §1352, *Limitation on use of appropriated funds to influence certain Federal contracting and financial transactions* – Prohibits the use of Federal funds in lobbying members and employees of Congress, as well as employees of Federal agencies, with respect to the award or amendment of any Federal grant, cooperative agreement,

contract, or loan. FEMA and DHS have codified restrictions upon lobbying at 44 CFR Part 18 and 6 CFR Part 9. (Refer to form included in application package.)

- *Drug-free Workplace Act*, as amended, 41 U.S.C. §701 et seq. – Requires the recipient to publish a statement about its drug-free workplace program and give a copy of the statement to each employee (including consultants and temporary personnel) who will be involved in award-supported activities at any site where these activities will be carried out. Also, place(s) where work is being performed under the award (i.e., street address, city, state and zip code) must be maintained on file. The recipient must notify the Grants Officer of any employee convicted of a violation of a criminal drug statute that occurs in the workplace. For additional information, see 44 CFR Part 17.
- *Debarment and Suspension* – Executive Orders 12549 and 12689 provide protection from fraud, waste, and abuse by debarring or suspending those persons that deal in an irresponsible manner with the Federal government. The recipient must certify that they are not debarred or suspended from receiving Federal assistance. For additional information, see 44 CFR Part 17.
- *Federal Debt Status* – The recipient may not be delinquent in the repayment of any Federal debt. Examples of relevant debt include delinquent payroll or other taxes, audit disallowances, and benefit overpayments. (OMB Circular A-129) (Refer to SF 424, item number 17.)
- *Hotel and Motel Fire Safety Act of 1990* – In accordance with section 6 of the *Hotel and Motel Fire Safety Act of 1990*, 15 U.S.C. §2225a, the recipient agrees to ensure that all conference, meeting, convention, or training space funded in whole or in part with Federal funds, complies with the fire prevention and control guidelines of the *Federal Fire Prevention and Control Act of 1974*, 15 U.S.C. §2225.

Grantees must comply with all regulations, guidelines, and standards adopted under the above statutes.

5.6 – 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 funding from FEMA. In addition, Executive Order 13347, *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 encourage consideration of the needs of individuals with

disabilities served by State, local, and tribal governments in emergency preparedness planning.

FEMA 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:

- **Comprehensive Preparedness Guide 301 (CPG-301): Interim Emergency Management Planning Guide for Special Needs Populations.** CPG-301 is designed to aid tribal, State, territorial, and local governments in planning for individuals with special needs. CPG-301 outlines special needs considerations for: Developing Informed Plans; Assessments and Registries; Emergency Public Information/Communication; Sheltering and Mass Care; Evacuation; Transportation; Human Services/Medical Management; Congregate Settings; Recovery; and Training and Exercises. CPG-301 is available at <http://www.fema.gov/pdf/media/2008/301.pdf>.
- **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 Federal, State, and local 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 LLIS.gov, you can request membership by registering online.

5.7 – Environmental Planning and Historic Preservation (EHP) Compliance. FEMA is required to consider the potential impacts to the human and natural environment of projects proposed for FEMA grant funding. FEMA, through its

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*, the *Clean Water 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 low-income and minority populations.

The grantee shall provide all relevant information to FEMA's Grant Programs Directorate (GPD) to ensure compliance with applicable Federal EHP requirements. Any project with the potential to impact natural or biological resources or historic properties cannot be initiated until FEMA has completed the required EHP review. In addition to a detailed project description that describes what is to be done with the grant funds, how it will be done, and where it will be done, grantees shall provide detailed information about the project (where applicable), including, but not limited to, the following:

- Project location (i.e., exact street address or map coordinates)
- Total extent of ground disturbance and vegetation clearing
- Extent of modification of existing structures
- Construction equipment to be used, staging areas, etc.
- Year that any affected buildings or structures were built
- Natural, biological, and/or cultural resources present within the project area and vicinity, including wetlands, floodplains, geologic resources, threatened or endangered species, or National Register of Historic Places listed or eligible properties, etc.
- Visual documentation such as good quality, color and labeled site and facility photographs, project plans, aerial photos, maps, etc.
- Alternative ways considered to implement the project (not applicable to procurement of mobile and portable equipment)

For projects that have the potential to impact sensitive resources, FEMA must consult with other Federal, State, and tribal 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 the protection and/or management of natural and cultural resources, including Federally-recognized Indian tribes, Tribal Historic Preservation Offices, and the Department of the Interior, Bureau of Indian Affairs. For projects with the potential to have adverse effects on the environment and/or historic properties, FEMA's EHP review process 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. Grantees who are proposing communication tower projects are encouraged to complete their Federal Communications Commission (FCC) EHP process prior to preparing their EHP review materials for GPD, and to include their FCC EHP materials with their submission to GPD. Completing the FCC process first and

submitting all relevant EHP documentation to GPD will help expedite FEMA's review.

Because of the potential for 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 grant funds toward the costs of preparing such documents. The use of grant funds for mitigation or treatment measures that are not typically allowable expenses will be considered on a case-by-case basis. Failure of the grantee to meet Federal, State, local, and territorial EHP requirements, obtain required 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.

Recipients shall not undertake any project without the prior approval of GPD, and must comply with all conditions placed on the project as the result of the EHP review. Any change to the approved project description will require re-evaluation for compliance with these EHP requirements. If ground disturbing activities occur during project implementation, the recipient must ensure monitoring of ground disturbance, and if any potential archeological resources are discovered, the recipient will immediately cease construction in that area and notify their GPD Program Analyst, and the appropriate State Historic Preservation Office. Any projects that have been initiated prior to approval will result in a non-compliance finding and will not be eligible for funding.

For more information on FEMA's EHP requirements, grant recipients should refer to FEMA's Information Bulletin #329, *Environmental Planning and Historic Preservation Requirements for Grants*, available at <http://www.fema.gov/pdf/government/grant/bulletins/info329.pdf>. Additional information and resources can also be found at <http://www.fema.gov/plan/ehp/ehp-applicant-help.shtm>.

5.8 – Royalty-free License. Applicants are advised that FEMA reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, or otherwise use, and authorize others to use, for Federal government purposes: (a) the copyright in any work developed under an award or sub-award; and (b) any rights of copyright to which an award recipient or sub-recipient purchases ownership with Federal support. Award recipients must agree to consult with FEMA regarding the allocation of any patent rights that arise from, or are purchased with, this funding.

5.9 – FEMA GPD Publications Statement. Applicants are advised that all publications created with funding under any grant award shall prominently contain the following statement: "This document was prepared under a grant

from the Federal Emergency Management Agency's Grant Programs Directorate (FEMA/GPD) within the U.S. Department of Homeland Security. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position or policies of FEMA/GPD or the U.S. Department of Homeland Security."

5.10 – Equipment Marking. Awardees may consider marking equipment in the following manner, "Purchased with funds provided by the U.S. Department of Homeland Security," in order to facilitate their own audit processes, as well as Federal audits and monitoring visits, which may result from receiving Federal funding. Equipment maintenance requirements are outlined in 44 CFR Part 13.32.

5.11 – Disadvantaged Business Requirement. Applicants are advised that, to the extent that recipients of a grant use contractors or subcontractors, such recipients shall use small, minority, women-owned or disadvantaged business concerns and contractors or subcontractors to the extent practicable.

5.12 – National Preparedness Reporting Compliance. *The Government Performance and Results Act of 1993* (Public Law 103-62) (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. FEMA anticipates using this information to inform future-year grant program funding decisions. Award recipients must agree to cooperate with any assessments, national evaluation efforts, or information or data collection requests, including, but not limited to, the provision of any information required for the assessment or evaluation of any activities within their grant agreement. This includes any assessments, audits, or investigations conducted by DHS, the Office of the Inspector General, or the U.S. Government Accountability Office (GAO).

C. 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). Any reports or documents prepared as a result of this grant shall be in compliance with Federal "plain English" policies, directives, etc. Please note that PARS contains edits that will prevent access to funds if reporting requirements are not met on a timely basis.

- 1. Federal Financial Report (FFR) – required quarterly.** Obligations and expenditures must be reported on a quarterly basis through the FFR (SF-425), which is due within 30 days of the end of each calendar quarter (e.g., for the quarter ending March 31, the FFR 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 FFR is due 90 days after the end date of the performance period.

OMB has directed that the FFR SF-425 replace the use of the SF-269, SF-269A, SF-272, and SF-272A, which are no longer available as of October 1, 2009. The SF-425 is intended to provide Federal agencies and grant recipients with a standard format and consistent reporting requirements throughout the government.

FFRs **must be filed online** through PARS.

Reporting periods and due dates:

- October 1 – December 31; *Due January 30*
- January 1 – March 31; *Due April 30*
- April 1 – June 30; *Due July 30*
- July 1 – September 30; *Due October 30*

- 2. Semi-Annual Assistance Progress Report (SAPR).** Following an award, the awardees will be responsible for providing updated obligation and expenditure information on a semi-annual basis. The applicant is responsible for completing and submitting the SAPR reports.

The SAPR 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 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.

SAPRs must be filed online at <https://grants.ojp.usdoj.gov>. Guidance and instructions can be found at <https://grants.ojp.usdoj.gov/gmsHelp/index.html>.
Required submission: SAPR (due semi-annually).

- 3. Exercise Evaluation and Improvement.** Exercises, implemented with grant funds, should be capabilities and performance-based and should evaluate performance of the targeted capabilities required to respond to the exercise scenario. Guidance related to exercise evaluation and the implementation of improvements is defined in the Homeland Security Exercise and Evaluation Program located at <https://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 the FEMA Grants and preparedness Community of Interest (COI) on the Homeland Security Information Network (HSIN) within 90 days following completion of the exercise.

The AAR documents the demonstrated performance of targeted capabilities and identifies recommendations for improvements. The IP outlines an exercising jurisdiction(s) plan to address the recommendations contained in the AAR. At a minimum, the IP must identify initial action items and be included in the final AAR. Guidance for the development of AARs and IPs is provided in the HSEEP manual.

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 GAO's *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 FY 2010 FRSGP 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. 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. Programmatic monitoring may also include the Regional Federal Preparedness Coordinators, when appropriate, to ensure consistency of project investments with regional and national goals and policies, as well as to help synchronize similar investments ongoing at the Federal, State, and local levels.

Monitoring will be accomplished through a combination of desk-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.

- 6. Grant Close-Out Process.** Within 90 days after the end of the period of performance, grantees must submit a final FFR and final SAPR detailing all accomplishments throughout the project. After these reports have been reviewed and approved by FEMA, a close-out notice will be completed to close out the grant.

The notice will indicate the project as 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 FFR. The grantee is responsible for returning any funds that have been drawn down but remain as unliquidated on grantee financial records.

Required submissions: (1) final SF-425, due 90 days from end of grant period; and (2) final SAPR, due 90 days from the end of the grant period.

PART VII.

FEMA CONTACTS

This section describes several resources that may help applicants in completing a FEMA grant application.

- 1. Centralized Scheduling and Information Desk (CSID).** CSID is a non-emergency comprehensive management and information resource developed by DHS for grants stakeholders. CSID provides general information on all FEMA grant programs and maintains a comprehensive database containing key personnel contact information at the Federal, State, and local levels. CSID can be reached by phone at (800) 368-6498 or by e-mail at ASKCSID@dhs.gov, Monday through Friday, 8:00 AM – 6:00 (EST).
- 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. Additional guidance and information can be obtained by contacting the FEMA Call Center at (866) 927-5646 or via e-mail to ASK-GMD@dhs.gov.
- 3. National Exercise Division (NED).** The NED within the FEMA National Preparedness Directorate maintains program management for the Homeland Security Exercise and Evaluation Program (HSEEP). All questions pertaining to HSEEP may be addressed to hseep@fema.gov or contact the NED at (202) 786-9873.
- 4. Homeland Security Preparedness Technical Assistance Program (HSPTAP) and Planning Support.** The HSPTAP provides direct support 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 prevent, protect against, respond to, and recover from terrorist and all hazard threats. In addition to the risk assessment assistance already being provided, FEMA also offers a variety of other direct support assistance programs.

The HSPTAP also provides access to planning support. The planning support aids jurisdictions by increasing their understanding of the complex issues faced in planning for various hazards and threats. This support includes leveraging subject-matter experts from around the country as well as enabling knowledge transfer from jurisdiction to jurisdiction.

More information can be found at http://www.fema.gov/about/divisions/pppa_ta.shtm or by e-mailing FEMA-TARequest@fema.gov or NPD-planning@dhs.gov.

5. **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 homeland security officials, as well as an updated list of homeland security exercises, events, and conferences. Additionally, LLIS includes online collaboration tools, including secure email and message boards, where users can exchange information. LLIS uses strong encryption and active site monitoring to protect all information housed on the system. The LLIS website can be found at: <http://www.LLIS.gov>.

6. **Information Bulletins.** Information Bulletins (IBs) provide important updates, clarifications, and policy statements related to FEMA preparedness grant programs. Grantees should familiarize themselves with the relevant publications. Information Bulletins can be found at: <http://www.fema.gov/government/grant/bulletins/index.shtm>.
7. **Information Sharing Systems.** FEMA encourages all State, regional, local, and tribal entities using FY 2010 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.
8. **U.S. General Services Administration's (GSA's) State and Local Purchasing Programs.** The 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**
Cooperative Purchasing, authorized by statute, allows State and local governments to purchase a variety of supplies (products) and services under specific GSA Schedule contracts to save time, money, and meet their everyday needs and missions.

The Cooperative Purchasing program allows State and local governments to purchase alarm and signal systems, facility management systems, firefighting and rescue equipment, law enforcement and security equipment, marine craft and related equipment, special purpose clothing, and related services off of Schedule 84 and Information Technology products and professional services

off of Schedule 70 and the Consolidated Schedule (containing IT Special Item Numbers) **only**. Cooperative Purchasing for these categories is authorized under Federal law by the *Local Preparedness Acquisition Act* (Public Law 110-248) and Section 211 of the *E-Government Act of 2002* (Public Law 107-347).

Under this program, State and local governments have access to GSA Schedule contractors who have voluntarily modified their contracts to participate in the Cooperative Purchasing program. The GSA 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 GSA to provide State and local governments the use of ALL GSA Federal Supply Schedules 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.

Products and services being purchased to facilitate recovery from one of the above listed events, may be purchased both in advance of and in the aftermath of a major disaster, as long as the products and services being purchased, will 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 contractors on GSA's website, <http://www.gsaelibrary.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/csd> to find a local customer service director in your area. For assistance at the national level, contact Tricia Reed at tricia.reed@gsa.gov or (571) 259-9921. More information is available on all GSA State and local programs at: www.gsa.gov/stateandlocal.

PART VIII. OTHER INFORMATION

A. Investment Justification Template

Investment Heading	
Organization/ Company Name	
Date of Application	
High Threat Urban 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 as applicable.	
Response Type	Narrative
Page Limit	Not to exceed 2 pages
Response Instructions	Describe the following: <ul style="list-style-type: none"> • Infrastructure (e.g. describe assets such as bridges, tunnels, yards, facilities, operational centers, etc); • Number of track miles; • Number of rail cars (differentiating tank cars); • Type and amount of SSM as defined for this grant, transported through High Threat Urban Areas annually. (Include separately the type and amount of TIH transported in tank cars and the type and amount of TIH transported by bulk loads.) • System maps, including listing of High Threat Urban Areas serviced; and, • Other sources of funding being leveraged for security enhancements. • For bridge projects, please provide the following information: <ul style="list-style-type: none"> ○ Asset Name

	<ul style="list-style-type: none"> ○ Owner/Operator ○ Complete Address ○ Latitude/ Longitude ○ County or Counties: ○ Local Government(s): ○ Identify public venues within 2.5 mile radius ○ Identify high density structures within a 2.5 mile radius (schools, hospitals, prisons, high rises, etc.) ○ Are there other back-ups or reroutes for the loss of this asset? List these backups, contingencies and redundancies. ○ Describe facilities that share perimeter boundaries with this asset? ○ Please identify other railroads utilizing this asset? ○ Is this asset part of a STRACNET route or STRACNET connector route? ○ What railroad division/subdivision is the asset part of? ○ Is this bridge fixed or moveable? ○ If moveable, what type? (Swing, Lift, Bascule) ○ What is the total length of the bridge? ○ What is the height of the bridge above mean water level? ○ Does the bridge cross a navigable waterway? Name waterway. ○ What is maximum permissible speed over bridge? ○ What is the average daily total of all trains? ○ What is the average daily volume of passenger trains? ○ Primary commodities carried by this bridge? ○ How many tracks on the bridge? ○ How often are underwater inspections of piers completed? ○ How often is an inspection of the bridge completed? ○ What is the primary alternate route if this bridge is out of service? Describe. ○ Are there bridge piers accessible by foot or vehicular traffic? ○ Is the bridge manned? What hours? ○ Does this bridge also carry public vehicular or foot traffic? ○ Has the bridge design or construction provided for risk mitigation, such as fire- proofing, non-flammable, etc.? ○ What are the million gross ton miles annually on this bridge? ○ What is the AAR security classification of this asset? ○ Maximum car weight permitted (in tons)?
Response	

II. Impact

II.A. Provide an abstract for this investment.	
Response Type	Narrative
Page Limit	Not to exceed 2 pages
Response Instructions	<ul style="list-style-type: none"> ● Describe the project, how it will be executed (e.g. expected implementation timeframe), and its purpose as it relates to the requirements outlined in Part I. ● Describe the specific needs and/or resource limitations that need to be addressed; ● Identify any potential partners (excluding specific vendors) and their roles and staffing requirements, and provide information on any existing agreements such as Memoranda of Understanding (MOU); ● Identify/provide an overview of the following, as applicable: <ul style="list-style-type: none"> ○ Equipment needs (e.g., number of GPS units and rail cars.) ○ Training needs (e.g., total number of employees, number of people to be trained, length of training, type of training, etc);

	<ul style="list-style-type: none"> ○ Planning needs (e.g., need to create/update vulnerability assessment/security plan to be compliant) ● Describe progress made on the security project this investment will be completing, if applicable; ● Reference use of prior year grant funds, if applicable; and, ● Describe how the project will be sustained during and after the period of performance of the grant. <ul style="list-style-type: none"> ○ <i>Note: Ensure that details on purchases within this section match what is outlined in the detailed budget.</i>
Response	

II.B. 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"> ● Identify the type of project (GPS, Vulnerability Assessment/Security Plan, Training/Exercise, Bridge Infrastructure Hardening ● 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; , ● Define the vision, goals, and objectives for the risk reduction, and summarize how the proposed investment will fit into the overall effort to meet the Federal security priorities (including integration into existing security protocols);
Response	

II.C. Vulnerability assessments and security plan information, as applicable.	
Response Type	Narrative
Page Limit	Not to exceed 2 pages
Response Instructions	<p>Please explain the status of your current vulnerability assessment and security plan with regard to the guidelines specified in Part I of the guidance. 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. If there are aspects of your current vulnerability assessment and security plan that do adhere to the guidelines in Part I, please describe those aspects.</p> <ul style="list-style-type: none"> ● If you are using a DHS approved methodology to complete your vulnerability assessment and security plan please specify which methodology you intend to use. ● If you are not using a DHS approved methodology to conduct your vulnerability assessment, address how your chosen methodology will comply with the vulnerability assessment and security plan requirements as listed in Part A. ● DHS may require the applicant to submit the entire vulnerability assessment tool/methodology requested above.
Response	

II.D. Training Program, as applicable.	
Response Type	Narrative
Page Limit	Not to exceed 2 pages
Response Instructions	<p>Describe the following about your current training program:</p> <ul style="list-style-type: none"> ● Number of staff including railroad front line employees. ● Type of staff, including employment titles. ● The number of employees who have received basic security awareness or other training in the past two years. <p>Describe the following about your proposed investment</p>

	<ul style="list-style-type: none"> • Number of railroad front line employees intended to be trained and the name of their employer (e.g. X front line employees work for Company A, Y front line employees work for Company B, etc, if applicable). • Type of training for the railroad front line employees, including summary course descriptions and how those courses adhere to the guidelines as listed in Part I of the guidance. • Length of training (e.g., 4 hours). • Number of printed materials consumed over the course of the training. • Number of companies and staff members involved in any exercise planning, execution, and review, if applicable. <p>Please provide information about how close the training program 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. Also please explain how you intend to provide refresher training and sustain the training program after the grant has expired.</p>
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 2010 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 2010 FRSGP) will be leveraged for this Investment. <p><i>Note: Investments will be evaluated on the expected impact on security relative to the amount of the investment (i.e., cost appropriateness). An itemized Budget Detail Worksheet and Budget Narrative must also be completed for this investment</i></p>
Response	

The following template illustrates how the applicants should indicate the amount of FY 2010 FRSGP funding required for the Investment, how these funds will be allocated across the cost elements, and any match being offered:

	Federal Request Total	Other Funding Sources	Grand Total
<i>Vulnerability Assessment/ Security Plan Development</i>			
<i>Training/Exercises</i>			
<i>Equipment</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. <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"> • 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 2010 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. However the timelines should convey that all critical processes have been considered and there is a plan in place to achieve those milestones (e.g. for training requests, courses conducted/ attended per month, number of railroad front line employees trained per class, etc.) • 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	

B. Sample Budget Detail Worksheet

Purpose. The Budget Detail Worksheet may be used as a guide to assist applicants in the preparation of the 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.

Name/Position	Computation	Cost
		\$
Total Personnel		\$

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.

Name/Position	Computation	Cost
		\$
Total Fringe Benefits		\$

C. Travel. Itemize travel expenses of project personnel by purpose (e.g., staff to training, field interviews, advisory group meeting, etc.). Show the basis of computation (e.g., six people to 3-day training at \$X airfare, \$X lodging, \$X subsistence). In training projects, travel and meals for trainees should be listed separately. Show the number of trainees and unit costs involved. Identify the location of travel, if known. Indicate source of Travel Policies applied, Applicant or Federal Travel Regulations.

Purpose of Travel	Location	Item	Computation	Cost
				\$
Total Travel				\$

D. Equipment. List non-expendable items that are to be purchased. Non-expendable equipment is tangible property having a useful life of more than one year. (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 rapid technical advances. Rented or leased equipment costs should be listed in the "Contractual" category. Explain how the equipment is necessary for the success of the project. Attach a narrative describing the procurement method to be used.

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

Item	Computation	Cost
		\$
Total Equipment		\$

E. Supplies. List items by type (office supplies, postage, training materials, copying paper, and other expendable items such as books, hand held tape recorders) and show the basis for computation. (Note: Organization's own capitalization policy and threshold amount for classification of supplies may be used). Generally, supplies include any materials that are expendable or consumed during the course of the project.

Supply Items	Computation	Cost
		\$
Total Supplies		\$

F. Consultants/Contracts. Indicate whether applicant's formal, written Procurement Policy or the Federal Acquisition Regulations are followed.

Consultant Fees: For each consultant enter the name, if known, service to be provided, hourly or daily fee (8-hour day), and estimated time on the project.

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

Name of Consultant	Service Provided	Computation	Cost
			\$
Subtotal – Consultant Fees			\$

Consultant Expenses: List all expenses to be paid from the grant to the individual consultant in addition to their fees (i.e., travel, meals, lodging, etc.)

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

Item	Location	Computation	Cost
			\$
Subtotal – Consultant Expenses			\$

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.

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

Item	Cost
	\$
Subtotal – Contracts	\$
Total Consultants/Contracts	\$

G. Other Costs. List items (e.g., reproduction, 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.

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.

Description	Computation	Cost
		\$
Total Other		\$

H. 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 Indirect Costs		\$

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.

Budget Category	Federal Amount	Non-Federal Amount
A. Personnel	\$	\$
B. Fringe Benefits	\$	\$
C. Travel	\$	\$
D. Equipment	\$	\$
E. Supplies	\$	\$
F. Consultants/Contracts	\$	\$
G. Other	\$	\$
H. Indirect Costs	\$	\$

Total Requested Federal Amount	Total Non-Federal Amount
\$	\$
Combined Total Project Costs	
\$	

C. Vulnerability Assessment and Security Plan Certification Statement

Vulnerability Assessment and Security Plan Certification Statement

Railroad carriers that have already completed a vulnerability assessment and developed and implemented a security plan that meet the requirements can use the statement below 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 the FY 2010 Freight Rail Security Grant Program Guidance and Application Kit. This security plan includes all elements required as listed in the FY 2010 Freight Rail Security Grant Program Guidance and Application Kit.

Signature

Date

Vulnerability Assessment and Security Plan Certification Statement 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 the statement below 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

D. Owner and Offerors Concurrence Statement

Owner and Offerors Concurrence Statement

Security sensitive materials offerors who ship by railroad and owners of railroad cars used in the transportation of security-sensitive materials may use grant funds received under this program to acquire and install satellite GPS tracking on rail cars that transport poisonous-by-inhalation/toxic inhalation hazardous (TIH) materials as defined in Part III.A. of the FY 2010 FRSGP guidance. Offerors applying for FY 2010 grant funding for GPS tracking can use the statement below to certify that the owner of the rail car acknowledges the grant application for the procurement of GPS tracking to attach to their rail car. Offerors applying for grant funds must submit this certification as part of their grant application.

I, [insert name], as [insert title] of [insert name of company], certify that I have informed the owner of the rail cars to which GPS equipment may be attached as a result of this grant application. I certify that I will take full responsibility for the acquisition, installation and maintenance of the system.

Offeror Signature _____ Date _____

Offeror Printed Name _____

Address _____

I, [insert name], as [insert title] of [insert name of company], certify that I have been informed by the sensitive security material offeror of their desire to attach GPS tracking equipment to rail cars which I own and they operate. I also certify that I approve of the installation of the GPS tracking equipment on the specified rail cars.

Owner Signature _____ Date _____

Owner Printed Name _____

Address _____

E. Other

Requirements Specific to For-Profit Entities

For-profit organizations are eligible to apply for funding under the FRSGP. The following requirements apply specifically to for-profit entities receiving Federal funding from FEMA:

1. Recipients of FRSGP funds must comply with the contract cost principles as defined in the Federal Acquisition Regulations (FAR), Part 31.2 Contract Cost Principles and Procedures, Contracts with Commercial Organizations
2. For purposes of financial and procedural administration of the FRSGP, recipients must comply with 2 CFR Part 215, Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Nonprofit Organizations (OMB Circular A-110) will apply, excluding Sections 40-48.
3. Recipient of FRSGP funds agree that this award may be terminated in accordance with 2 CFR Part 215.61. If the Federal Government determines that a grant will be terminated, it will be carried out in accordance with the process specified in Part 49 of the FAR.
4. Recipients of FRSGP funds may not make a profit as a result of this award or charge a management fee for the performance of this award.
5. Recipients of FRSGP funds must have a financial audit and compliance audit performed by qualified individuals who are organizationally, personally, and externally independent from those who authorize the expenditure of Federal funds. This audit must be performed in accordance with the United States Government Accountability Office Government Auditing Standards. The audit threshold contained in OMB Circular A-133 applies. This audit must be performed on a program-wide basis to ascertain the effectiveness of financial management systems and internal procedures that have been established to meet the terms and conditions of the award. The management letter must be submitted with the audit report. Recipient audit reports must be submitted no later than nine (9) months after the close of each fiscal year during the term of the award. The distribution of audit reports shall be based on requirements in the current edition of 2 CFR Part 215, Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations (OMB Circular A-110). Note: If your audit disclosed findings or recommendations, you must include with your audit report a corrective action plan containing the following: (1) The name and number of the contact person responsible for the corrective action plan; (2) specific steps taken to comply with the recommendations; (3) a timetable for performance or implementation dates for each recommendation; and (4) descriptions of monitoring to be conducted to ensure implementation.

Helpful Hints for Applicants:

Are the following components included in the application package?

- SF 424, SF 424A, SF 424B, SF LLL
- Investment Justifications for projects
- Detailed budgets containing only allowable costs
- Vulnerability Assessment/Security Plan Certification (if applicable)

Are the following items addressed within the Investment Justification narratives and detailed budgets?

- Do the IJ and the detailed budget only include allowable costs?
 - Are all of the expenses in the detailed budget addressed in the IJ narrative? (for example, a camera equipment budget line item should be addressed in narrative form in the IJ as it pertains to the overall security program)
 - Does the information in the detailed budget align with the budget summary in the IJ narrative?
- Does the IJ clearly explain how the projects fit into a funding priority area (as identified in Part I)?
- Does the IJ discuss how this investment will specifically address one or more of the funding priorities identified in the current year's grant guidance?
- Does the IJ discuss how this investment will decrease or mitigate risk?
- Is the cost effectiveness of the project clearly explained in the IJ? How does this project provide a high security return on investment?
- Are timelines realistic and detailed?
- Are possible hurdles addressed in a clear and concise fashion?
- Does the M&A total no more than five percent (5%) of the total award?