FISCAL YEAR 2011

FREIGHT RAIL SECURITY GRANT PROGRAM

GUIDANCE AND APPLICATION KIT
SECTION I – APPLICATION AND REVIEW INFORMATION

MAY 2011

U.S. DEPARTMENT OF HOMELAND SECURITY

Title of Opportunity: Fiscal Year (FY) 2011 Freight Rail Security Grant Program (FRSGP)

Funding Opportunity Number: DHS-11-GPD-075-000-01

Catalog of Federal Domestic Assistance (CFDA) Number: 97.075

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. EDT, June 20, 2011.**

Additional Overview Information:

- **Reformatted FRSGP Guidance Kit.** Due to continued stakeholder feedback and recommendations, Grant Programs Directorate (GPD) has reformatted its FY 2011 FRSGP Guidance and Application Kit. The Kit is now structured into two separate documents, referred to as *Section I* and *Section II.* While both are important documents for grantees to study and thoroughly familiarize themselves with, *Section I* is intended to help grantees during the application phase of the FRSGP, whereas *Section II* is intended to help grantees in understanding the rules and regulations associated with administering federally-funded grant awards.

- **Enhanced Data Collection.** As part of the DHS Performance Management Initiatives, including the Quadrennial Homeland Security Review (QHSR) Report, FEMA will enhance data collection processes and tools to assess the use and impact of FY 2011 FRSGP grant funds. Grantees will not be asked to provide additional data, but may be required to modify existing data reporting processes to collect more useful performance information.

- **Sensitive Security Information (SSI) Requirements.** For the purposes of the Freight Rail Security Grant Program, all Investment Justifications (IJ) shall be considered SSI and treated as such. This means labeling as SSI and password protecting appropriate documents prior to submission. The passwords for protected documents must be sent (separate of the documents) to the following e-mail address AskCSID@dhs.gov

  The subject line of the email should identify:
  - Applicant name
  - Application number

  The body of the e-mail should clearly identify:

- Applicant name
- IJ number and/or summary description
- State
- POC information

NOTE: A single password should be provided for all SSI documents within the same application.

Further information regarding these requirements can be found on page 31.

CONTENTS

PART I.
FUNDING OPPORTUNITY DESCRIPTION

The Fiscal Year (FY) 2011 Freight Rail Security Grant Program (FRSGP) is a component of the Transit Security Grant Program (TSGP), one of five DHS grant programs that 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. FRSGP provides funds to freight railroad carriers, owners and offerors of railroad cars, and owners of rail bridges to protect critical surface transportation infrastructure from acts of terrorism and increase resiliency of the freight rail system. The FY 2011 FRSGP is authorized by section 1513 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Public Law 110-53) (hereafter "9/11 Act") and the *Department of Defense and Full-Year Continuing Appropriations Act, 2011* (Public Law 112-10).

The funding priorities for the FY 2011 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 (EOs), 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. 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/files/publications/gc_1189788256647.shtm*.

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 2011 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 intelligence information and risk/vulnerability assessments; ranking and rating rail and mass transit assets nationwide against threats associated with potential terrorist attacks; and 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
The FY 2011 FRSGP is authorized by section 1513 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Public Law 110-53) and the *Department of Defense and Full-Year Continuing Appropriations Act, 2011* (Public Law 112-10).

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. For more information on grant extensions, see *Section II, Part I.A.*

Available Funding
In FY 2011, the total amount of funds distributed under this grant program will be $10,000,000.

Cost Match
The FY 2011 FRSGP has a 75 percent (75%) Federal and 25 percent (25%) grantee cost match cash- or in-kind match requirement as defined under 44 CFR §13.24. Vulnerability assessments and security plans are exempt from this cost match requirement.

FEMA administers cost sharing requirements in accordance with 44 CFR Part §13.24. To meet matching requirements, the grantee contributions must be reasonable, allowable, allocable, and necessary under the grant program and must comply with all Federal requirements and regulations.

A. Funding Priorities

The funding priorities for the FY 2011 FRSGP reflect the Department's overall investment strategy as well as requirements of the 9/11 Act. The key goals of the FY 2011 FRSGP are to establish the basis for capital security improvements by funding vulnerability assessments and security plans, training to frontline personnel, security-related exercises, global positioning system (GPS) tracking on railroad cars, and infrastructure hardening on rail bridges. 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 2011 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 *Section I, Part II.B*. Please note that the activities allowed under the following funding priorities constitute Sensitive Security Information (SSI). Information submitted in the course of applying for funding or reporting under certain programs or provided in the course of an entity's grant management activities under those programs which is under Federal control is subject to protection under SSI, and must be properly identified and marked. SSI is a control designation used by DHS to protect information related to transportation security. This designation is applied to information about security programs, vulnerability and threat assessments, screening processes, technical specifications of certain screening equipment and objects used to test screening equipment, and equipment used for communicating security information relating to air, land, or maritime transportation. The applicable information is spelled out in greater detail in 49 CFR Part §1520.

1. **GPS tracking.** Owners and offerors[1] 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 2011 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.

   <u>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</u>. A concurrence statement can be found in *Section I, Part VI.D* 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. <u>All eligible applicants must submit the railcar identification numbers of the railcars on which they are planning to install GPS equipment</u>.

   Satellite tracking equipment must be able to meet specific communication protocol standards that are outlined in 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 Administration (TSA) as a condition of the award.

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

2. **Infrastructure hardening on rail bridges.** Owners of rail bridges that are used for freight rail transportation may apply for infrastructure hardening capabilities. 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. Additional information is available on page 18.

3. **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. 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 2011 FRSGP funds, see pages 29 - 30. 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 Part §172.802 may request funding to conduct a new vulnerability assessment and to develop a new security plan to meet the requirements listed in the 9/11 Act. If the applicant's current vulnerability assessment and security plan comply fully with the requirements of the FY 2011 FRSGP 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 *Section I, Part VI.C* and must be submitted as part of the application submission.

4. **Security training and exercises for railroad frontline employees.** Effective employee training programs address individual employee responsibilities and provide heightened security awareness. Training should cover assessment and reporting of incidents, employee response, crew communication and coordination, and incident evacuation procedures. For more information about the components of a training program to be completed with FY 2011 FRSGP funds, see pages 16 - 17. Note that adherence to these components is one factor in grant application evaluation.

Security exercises, either in conjunction with training or separately, are allowable. The exercises must be focused on antiterrorism. Exercises that are regionally collaborative and include 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 2011 FRSGP Guidance and Application Kit to be eligible for training. A certification form can be found in *Section I, Part VI.C* and must be submitted as part of the application submission.

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.

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 on page 14.

Eligible Class II and Class III freight railroad carriers that have completed a vulnerability assessment and security plan that comply with 49 CFR Part §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 requirements, 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 *Section I, Part VI.C* 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 below. 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.

Owners of railroad bridges may apply for funds for infrastructure hardening, including access control, lighting, intrusion detection, etc., for eligible bridges. Information on bridge eligibility is on page 18.

In order to request FY 2011 FRSGP funds, applicants must complete and submit an Investment Justification, the outline of which is provided in *Section I, Part VI.A.*.

GPS Tracking Requirements

GPS tracking projects are for the purpose of tracking 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 as well as related shipment data as defined by DHS
- The GPS tracking data obtained via the satellite GPS equipment is the property of the railcar owner, however, the railcar owner will allow DHS unrestricted access to the GPS tracking data as a condition of the grant award
- If the system supports geofencing, the system shall initiate transmission of current location and status data within 30 minutes of traversing a High Threat Urban Areas (HTUAs) boundary[2] and shall deliver that location and status information to the DHS-designated data communications gateway in the prescribed data formats within one hour of the railcar traversing the HTUA boundary. Additionally, each railcar will report its location and status at least once every 24 hours regardless of location.
- If the hardware does not support geofencing, the grantee will transmit the GPS current location and status data to DHS at an interval of every four hours regardless of its location. DHS will expect to receive this data within 30 minutes of transmission.
- If the hardware supports movement detection, the four hour reporting interval can be suspended after four hours of standstill time providing that a transmission is initiated to DHS within 30 minutes of the railcar resuming movement. The last reporting, prior to suspension of the four hour interval, must be codified as a "standstill event" as described herein.
- For the purposes of HTUA geo-fencing or reporting the HTUA location, overlapping HTUA area should be treated as one contiguous area. TSA will provide a specific code for each such area.
- The system must allow an authorized DHS representative to directly log in through a secure web portal to allow access viewing and downloading of shipment and GPS location data as defined by DHS. The grant recipient is responsible for protection of its proprietary data and limiting DHS access to only required data.
- The system shall support active polling of the rail car tracking units, including the capability for an authorized DHS representative to poll GPS-enabled TIH railcars for current location and status data by: Equipment Initial and Equipment Number, last reported location, last reported State, last reported county and/or by HTUA. Transmission to DHS will be made via a secure web portal, web service, or similar solution

[2] As defined by the U.S. Department of Homeland Security, Transportation Security Administration

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

Technology Standards

- The GPS tracking system shall meet all Federal, State, local, and industry safety standards regarding the installation and maintenance of GPS tracking equipment on grantees' TIH railcars. The tracking system shall be tested periodically and the results of the test recorded.
- The GPS tracking system shall be capable of meeting the operational requirements outlined above with respect to location accuracy and data timeliness
- The GPS tracking system shall support active polling of targeted GPS-enabled TIH railcars. The transmission of current location and status data to a DHS-designated data communications gateway must commence within 30 minutes of active polling.
- Grantees shall also provide a single point of contact to DHS that would be responsible for initiation of polling requests from DHS as conditions may require
- The active polling function shall include the capability for an authorized DHS representative to directly query (via active polling) GPS-enabled TIH railcars by Equipment Initial and Equipment Number or by HTUA code via a secure web portal, web service, or similar solution
- The Grantee is responsible for protection of its non-UCI data and limiting DHS access to only UCI data
- The GPS tracking system (hardware, software, and infrastructure) must be able to meet specific data content, accuracy guidance and communication protocol standards defined in the UCI and associated documents
- The GPS tracking system shall be tested periodically as defined in DHS/TSA guidelines by the grantee or the grantees' designee. The test criteria and results shall be recorded and be made available to DHS for review on request by an authorized DHS representative; test criteria and results must meet DHS requirements on review.

Data Requirements

- Transmission of data from GPS tracking systems via 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. UCI transmission enveloping, communications protocols, and encryption methods shall comply with DHS IT Security guidelines.
- Grant recipients will be expected to provide this GPS and shipment data on any railcar that is reported via a bill of lading to a rail carrier where the contents are defined by a RSSM-TIH STCC Code and the quantity of shipped material requires completion of the "LH" section of an EDI-404. If the rail car is empty and cleaned and not requiring a bill of lading with a hazardous materials information segment completed, it need not be tracked.

- All railcar GPS location and status reporting will be expected to be in local time, based on the rail cars location at the time of the reporting. The time zone codes listed in the UCI documentation will be required to denote the time zone.
- DHS shall periodically review and update the UCI definition to address emerging technology, industry, and government business needs and/or objectives

Communications Plan
A communications plan must be established to include Standard Operating Procedures (SOPs) 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 see *Section I, Part II.B* for information on funding guidelines. Applicants should send an email to AskCSID@dhs.gov for additional information.

Vulnerability Assessment Requirements
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 the following acts of terrorism: 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 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 – must take 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
    - 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 regarding the consequences and likelihood of success of an act of terrorism, and the 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 see *Section I, Part II.B* for information on funding guidelines.
Applicants should send an email to ASKCSID@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)"- A team responsible for developing, managing, and ensuring the security countermeasures are implemented in response to a security threat/incident
- Roles 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 if a threat exists (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 the railroad in response to a terrorist attack or increased threat
- 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 carriers 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
- Measures designed to ensure the 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 the railroad, cargo and cargo handling equipment owned by the customer, and other railroad interdependencies covered by contractual agreements
- Procedures to address secure handling and storage of TIH 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 a timeline
- 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 see *Section I, Part II.B* for information on funding guidelines.
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:

- Security Awareness
    - Identifying, reporting, and reacting to suspicious activity, suspicious items, dangerous substances, and security incidents
    - Determining the seriousness of an occurrence or threat
    - 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
    - Identifying and maintaining domain awareness of Rail Security Sensitive Material (RSSM) shipments and associated manifest paperwork
    - Understanding RSSM Chain of Custody Requirements
- Behavior Recognition
    - Recognizing behaviors associated with terrorists' reconnaissance and planning activities
    - Behavioral and psychological aspects of, and responses to, terrorist incidents, including the ability to cope with hijacker behavior
- Threat/Incident Prevention, Protection, and Response
    - Understanding individual roles and responsibilities in prevention of and response to terrorist attacks
    - Crew communication and coordination
    - Evacuation procedures for employees
    - Self defense and use of non-lethal defense devices
    - Use of personal protective devices and other protective equipment
    - Procedures for communicating and interacting with governmental and nongovernmental emergency response providers

- Operation and maintenance of security equipment and systems, to the extent the employee's responsibilities involve use or maintenance of such equipment
- 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 components:

- Threat/Incident Prevention, Protection, and Response:
  - Understanding the role of the operations control center in the prevention of, protection against and response to terrorist attacks
  - 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
  - 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
  - Specifying priorities in prevention of, protection against, detection of, deterrence of and response to a terrorist threat or attack
  - Directing and coordinating prevention, protection detection, deterrence, and response activities for terrorist threat or attack
  - 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
  - Use of personal protective devices and other protective equipment
  - Procedures for communicating and interacting with governmental and nongovernmental emergency response providers
  - Operation and maintenance of security equipment and systems
  - 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 will receive
- How many employees will be trained

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 see *Section I, Part II.B* for information on funding guidelines.
Applicants should send an email to TSAGrants@tsa.dhs.gov for additional information.

Infrastructure Hardening on Rail Bridges Requirements
To be eligible for infrastructure hardening funding, bridges must have a volume exceeding 4.9 million gross ton miles (MGTM). 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 2011 FRSGP.

Please see *Section I, Part II.B* for information on funding guidelines.
Applicants should send an email to TSAGrants@tsa.dhs.gov for additional information.

B. Funding Guidelines

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.

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.

The following pages outline general allowable and unallowable FRSGP costs guidance.

1. **Management and Administration (M&A).** FY 2011 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 2011 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

2. Allowable Costs. 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

Awardees must commit to minimum training standards to be set by the Department. 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:

GPS Tracking on Railroad Cars

- **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 section. Cost of additional sensory information is not eligible and, if included, must be assumed by the railroad car owner.

Vulnerability Assessments and Security Plans

FY 2011 FRSGP funds may be used by Class II and Class III railroad carriers for the development of vulnerability assessments and security plans.

Training and Exercise

FY 2011 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 *Section I, Part II.A* of the FY 2011 FRSGP Guidance and Application Kit.

- **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 an 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).
- **Other Items.** These costs may include space/location/facilities for exercise planning and conduct as well as rental of equipment (e.g., portable toilets, tents, food, and gasoline). Grantees are encouraged to use free public space/locations/facilities, whenever available, prior to the rental of space/locations/facilities. This may also include costs for signs, badges, and similar materials.

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.

3. **Unallowable Costs.** 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

PART III.
ELIGIBILITY INFORMATION

A. Eligible Applicants

Eligible applicants for the FY 2011 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, owners and offerors of railroad cars that transport TIH materials as defined in 49 CFR Part §171.8, and owners of rail bridges that have a volume exceeding 4.9 MGTM. 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 Part §173.50; (2) A tank car containing a material poisonous by inhalation as defined in 49 CFR Part §171.8, including anhydrous ammonia, Division 2.3 gases poisonous by inhalation as set forth in 49 CFR Part §173.115(c), and Division 6.1 liquids meeting the defining criteria in 49 CFR Part §173.132(a)(1)(iii) and assigned to hazard zone A or hazard zone B in accordance with 49 CFR Part §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 Part §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 2011 FRSGP 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 Part §172.802[3]

[3]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 the 9/11 Act

Table 1. FY 2011 Freight Rail Security High Threat Urban Areas (HTUA)

FY 2011 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 2011 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 *Section I, Part II.A*.** 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 Part §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 Part §171.8, including anhydrous ammonia but excluding residue quantities of these materials.
- Travel from, to or through a HTUA.

Please refer to *Section I, Part VI.C* for examples of certification statements. These statements must be submitted as part of the grant application, as applicable.

B. Governance

National Incident Management System (NIMS) Implementation

In accordance with 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 including voluntary 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 2010 NIMS implementation must be considered prior to allocation of any Federal preparedness awards in FY 2011. Since FY 2007, the National Integration Center (NIC) has advised State, Tribal nation, and local governments to self assess their respective progress relating to NIMS implementation objectives in the NIMS Compliance Assistance Support Tool (NIMSCAST).[4] 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*.

[4] 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 should update their respective NIMSCAST assessments and, if necessary, submit a Corrective Action Plan via NIMSCAST for FY 2010. Corrective Action Plans are only required if a jurisdiction fails to meet one of the NIMS implementation activities. Comprehensive information concerning NIMS implementation for States, Tribal nations, local governments, nongovernmental organizations, and the private sector is available through the NIC at FEMA's NIMS Resource Center at *www.fema.gov/nims*.

State, Tribal, and local governments should continue to implement NIMS training guidance (course curricula and instructor qualifications) contained in the *Five-Year NIMS Training Plan*, released in February 2008 and any successor guidance released by FEMA. [Note: Coursework and training developed and/or delivered by National Wildfire Coordinating Group (NWCG) meet the course and instructor requirements of the *Five-Year NIMS Training Plan*]. NIMS training guidance is available on FEMA's NIMS Resource Center at *www.fema.gov/emergency/nims/NIMSTrainingCourses*.

The primary grantee/administrator of FY 2011 FRSGP award funds is responsible for determining if sub-awardees have demonstrated sufficient progress in NIMS implementation to disburse awards.

PART IV.
APPLICATION AND SUBMISSION INFORMATION

A. Address to Request Application Package

FEMA makes all funding opportunities available on the Internet at *http://www.grants.gov*. If you experience difficulties accessing information or have any questions please call the Grants.gov customer support hotline at (800) 518-4726.

Application forms and instructions are available at Grants.gov. To access these materials, go to *http://www.grants.gov*, select "Apply for Grants," and then select "Download Application Package." Enter the 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."

B. Content and Form of Application

1. **Application via Grants.gov.** All applicants must file their applications using the Administration's common electronic "storefront" – *http://www.grants.gov*. Eligible grantees must apply for funding through this portal, accessible on the Internet at *http://www.grants.gov*.

   The application must be started and submitted using Grants.gov after Central Contractor Registration (CCR) is confirmed. The on-line application includes the following required form:

   - Standard Form 424, Application for Federal Assistance

   When applicants apply through *http://www.grants.gov*, the Standard Form 424 in the initial Grants.gov application will need to be submitted. The Standard Form 424 will be retrieved by ND Grants and the system will automatically populate the relevant data fields in the application. Because FEMA will need to conduct an initial review of the application prior to the submission deadline of June 20, 2011, grantees are encouraged to initiate and complete the Standard Form 424 submission within Grants.gov by **no later than June 13, 2011**. Upon the completion of the initial review, FEMA will determine whether an application should proceed further and the applicant will be notified to complete their submission by fulfilling additional

application requirements (e.g., budget, IJ, Work Plan, etc.) listed below by **no later than June 20, 2011**.

The application must be completed and final submission made through the ND Grants system located at *https://portal.fema.gov*. If you need assistance registering for the ND Grants system, please contact FEMA's Enterprise Service Desk at (888) 457-3362. Applicants are encouraged to begin their ND Grants registration at the time of solicitation to ensure they have adequate time to start and complete their application submission. The ND Grants system includes the following required forms and submissions:

- Standard Form 424A, Budget Information (Non-construction)
- Standard Form 424B, Standard Assurances (Non-construction)
- Standard Form 424C, Budget Information (Construction)
- Standard Form 424D, Standard Assurances (Construction)
- Standard Form LLL, Disclosure of Lobbying Activities (if the grantee has engaged or intends to engage in lobbying activities)
- Grants.gov (GG) Lobbying Form, Certification Regarding Lobbying
- FEMA Form 20-16C, Certifications Regarding Lobbying; Debarment, Suspension and Other Responsibility Matters; and Drug-Free Workplace Requirements
- Investment Justification (OMB Number 1660-0121/FEMA Form 089-6)
- Budget Detail Worksheet

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

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 *http://www.grants.gov* and for CCR. 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.** The application process also involves an updated and current registration by the applicant, which must be confirmed at *http://www.ccr.gov*.

4. **Investment Justification (IJ).** As part of the FY 2011 FRSGP application process, applicants must develop a formal IJ that addresses each initiative being proposed for funding. These IJs must demonstrate how proposed projects address gaps and deficiencies in current programs and capabilities. The IJ must demonstrate the ability to provide enhancements consistent with the purpose of the program and guidance provided by FEMA. Applicants must ensure that the IJ is consistent with all applicable requirements outlined in this application kit.

Applicants may propose up to four Investments within their application. A separate IJ must be submitted for each proposed project. All IJs must be submitted with the application by June 20, 2011.

The IJ 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 *http://www.grants.gov*, no later than 11:59 p.m. EST, June 20, 2011. Applicants must submit one SF-424 per application, as well as an IJ, 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

FY 2011 FRSGP applicants must provide responses to all questions. The noted page limits are suggestions only.

Investment Justification Submission and File Naming Convention
IJs must be submitted with the grant application as a file attachment within *https://portal.fema.gov* Applicants must use the following file naming convention when submitting IJs as part of the FY 2011 FRSGP:

IJ (through *https://portal.fema.gov*) ensure file attachment Company Name_IJ Number (Example: ABC Railroad_IJ#1).

Applicants will find a sample IJ worksheet in *Section I, Part VI.A*. This worksheet may be used as a guide to assist applicants in the preparation of the IJ.

Detailed Budget Submission and File Naming Convention
Detailed Budgets must be submitted with the grant application as a file attachment within *https://portal.fema.gov* Applicants must use the following file naming convention when submitting detailed budgets as part of the FY 2011 FRSGP:

Detailed Budget (through *https://portal.fema.gov*) ensure file attachment
Company Name_IJ Number_Budget (Example: ABC Railroad_IJ#1_Budget).

Applicants will find a sample Budget Detail Worksheet in *Section I, Part VI.B*. 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 *Section I, Part VI.C* 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 strengths and weaknesses, and the existing countermeasures and their level of effectiveness in reducing identified vulnerabilities. This can include:
     - 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
     - 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 that 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.

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 See *Section I, Part VI.C* 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
- Designation of "Rail Security Coordinator(s)"- Team responsible for developing, managing, and ensuring the security countermeasures are implemented in 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 in response to a security threat/incident
- Security countermeasures to be implemented by railroad in response to a terrorist attack or threat incident
- 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 the railroad, cargo and cargo handling equipment owned by the customer and other railroad interdependencies covered by contractual agreements
- Procedures to address secure handling and storage of TIH 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:
  - A list of outstanding vulnerabilities
  - Mitigation options and associated costs of alternatives
  - A preferred mitigation strategy
  - A 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/TIH materials as defined in *Section I, Part III.A* of the FY 2011 FRSGP Guidance and Application Kit. Offerors applying for FY 2011 grant funding for GPS tracking can use the statement in *Section I, Part VI.D* 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.

8. **Sensitive Security Information (SSI) Requirements.** Information submitted in the course of applying for funding or reporting under certain programs or provided in the course of an entity's grant management activities under those programs which is under Federal control is subject to protection under SSI, and must be properly identified and marked. SSI is a control designation used by the Department of Homeland Security related to protecting information related to transportation security. It is applied to information about security programs, vulnerability and threat assessments, screening processes, technical specifications of certain screening equipment and objects used to test screening equipment, and equipment used for communicating security information relating to air, land, or maritime transportation. The applicable information is spelled out in greater detail in 49 CFR Part §1520.7.

   For the purposes of the FRSGP, all IJs shall be considered SSI and treated as such. This means labeling as SSI and password protecting appropriate documents prior to submission. The passwords for protected documents must be sent (separate of the documents) to the following e-mail address AskCSID@dhs.gov

   The subject line of the email should identify:
   - Applicant name
   - Application number

   The body of the e-mail should clearly identify:
   - Applicant name
   - IJ number and/or summary description
   - State
   - POC information

   NOTE: A single password should be provided for all SSI documents within the same application.

C. Environmental Planning and Historic Preservation (EHP) Compliance

FEMA is legally required to consider the potential impacts of all grant-funded projects on environmental resources and historic properties. For FRSGP and other preparedness grant programs, this is accomplished via FEMA's EHP Review.

Grantees must comply with all applicable EHP laws, regulations, and EOs in order to draw down their FY 2011 FRSGP grant funds. Any project with the potential to impact natural resources or historic properties cannot be initiated until FEMA has completed the required FEMA EHP review. Grantees that implement projects prior to receiving EHP approval from FEMA risk de-obligation of funds.

Not all projects require a FEMA EHP review. For example, the following activities would not require a FEMA EHP review: planning and development of policies or processes; management, administrative or personnel actions; classroom-based training; table top exercises; and, acquisition of mobile and portable equipment (not involving installation). However, any proposed project funded through FRSGP that involves the installation of equipment or ground-disturbing activities must undergo the FEMA EHP review process.

If an EHP review is required, you will receive notification from your Program Analyst on the type of EHP documentation needed for the EHP review. In these instances, grantees must complete the FEMA EHP Screening Form (OMB Number 1660-0115/FEMA Form 024-0-01) and submit it, with all supporting documentation, to the GPD EHP team at GPDEHPInfo@fema.gov. Refer to Information Bulletins (IBs) 329, 345, and 356 (located at *http://www.fema.gov/government/grant/bulletins/index.shtm*) and *Section II, Part I.B.5.5.6* for further details on EHP requirements.

D. Submission Dates and Times

All submissions will be received by **no later than 11:59 p.m. EDT, June 20, 2011**. Late applications will neither be considered nor reviewed. Only applications started through *http://www.grants.gov* and completed through the ND Grants system located at *https://portal.fema.gov* will be accepted.

PART V.
APPLICATION REVIEW INFORMATION

A. Review Criteria

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 2011 FRGSP, and to help in submission of projects that will have the highest impact on reducing risks for freight railroad companies and their customers.

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 *Section I, 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 IJs 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 percent (20%).** Projects will be evaluated based on their adherence to the project type requirements listed in *Section I, Part II.A* of the guidance (e.g. vulnerability assessment requirements, security plan requirements, frontline employee training requirement, and GPS requirements)

2. **Cost Appropriateness – 20 percent (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 percent (20%).** Projects will be evaluated based on the assessed ability of the applicant to complete the proposed project within the allowed 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 percent (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 percent (30%).** DHS is committed to focusing the bulk of available funds on high-risk areas. As such, the risk associated with (1) HTUAs and (2) the type and amount of SSM including TIH materials hauled or stored will also be considered in the funding of the project.

B. Review and Selection Process

The FY 2011 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 IJs, budgets, required forms and certifications, and application process requirements.

Funds will not be made available for obligation, expenditure, or drawdown until the applicant's budget and budget narrative have been approved by FEMA.

The applicant must provide a detailed budget for the funds requested. The detailed budget must be submitted with the grant application as a file attachment within *http://www.grants.gov*. The budget must be complete, reasonable, and cost-effective in relation to the proposed project. The budget should provide the basis of computation of all project-related costs, any appropriate narrative, and a detailed justification of M&A costs.

C. Anticipated Announcement and Award Dates

FEMA will evaluate, act on applications, and make awards on or before September 30, 2011.

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*.

PART VI.
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: • 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: • 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: o Asset Name

	o Owner/Operator o Complete Address o Latitude/ Longitude o County or Counties: o Local Government(s): o Identify public venues within 2.5 mile radius o Identify high density structures within a 2.5 mile radius (schools, hospitals, prisons, high rises, etc.) o Are there other back-ups or reroutes for the loss of this asset? List these backups, contingencies and redundancies. o Describe facilities that share perimeter boundaries with this asset? o Please identify other railroads utilizing this asset? o Is this asset part of a STRACNET route or STRACNET connector route? o What railroad division/subdivision is the asset part of? o Is this bridge fixed or moveable? o If moveable, what type? (Swing, Lift, Bascule) o What is the total length of the bridge? o What is the height of the bridge above mean water level? o Does the bridge cross a navigable waterway? Name waterway. o What is maximum permissible speed over bridge? o What is the average daily total of all trains? o What is the average daily volume of passenger trains? o Primary commodities carried by this bridge? o How many tracks on the bridge? o How often are underwater inspections of piers completed? o How often is an inspection of the bridge completed? o What is the primary alternate route if this bridge is out of service? Describe. o Are there bridge piers accessible by foot or vehicular traffic? o Is the bridge manned? What hours? o Does this bridge also carry public vehicular or foot traffic? o Has the bridge design or construction provided for risk mitigation, such as fire- proofing, non-flammable, etc.? o What are the million gross ton miles annually on this bridge? o What is the AAR security classification of this asset? o 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	• 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: o Equipment needs (e.g., number of GPS units and rail cars.) o Training needs (e.g., total number of employees, number of people to

	be trained, length of training, type of training, etc); o 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. o *Note: Ensure that details on purchases within this section match what is outlined in the detailed budget.*
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	• 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	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. • 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	Describe the following about your current training program: • 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. Describe the following about your proposed investment • 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. 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.
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	• Complete the chart below to identify the amount of funding you are requesting for this Investment only; • Funds should be requested by allowable cost categories (as identified in the FY 2011 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 2011 FRSGP) will be leveraged for this Investment. *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*
Response	

The following template illustrates how the applicants should indicate the amount of FY 2011 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
Vulnerability Assessment/ Security Plan Development			
Training/Exercises			
Equipment			
M&A			
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	• 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	• 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. Up to 10 milestones may be provided.	
Response Type	Numeric and Narrative
Page Limit	Not to exceed 1 page
Response Instructions	• 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 2011 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. Any sole source contracts must follow the requirements set forth in 44 CFR Section 13.36.

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 2011 Freight Rail Security Grant Program Guidance and Application Kit. This security plan includes all elements required as listed in the FY 2011 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/ TIH materials as defined in Part III.A. of the FY 2011 FRSGP guidance. Offerors applying for FY 2011 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

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)
- Owner and Offeror Concurrences Statement (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 5 percent (5%) of the total award?