

Highway Infrastructure and Motor Carrier Modal Annex

Table of Contents

Highway Infrastructure and Motor Carrier Modal Annex

1	Executive Summary	-1
2	Overview of Mode	2
2.1	Vision of Mode	2
2.2	Description of Mode	2
2.3	GCC/SCC Structure and Process	3
3	Implementation Plan	7
3.1	Priorities and Programs.....	7
3.1.1	Priorities	7
3.1.2	Programs.....	12
3.2	Effective Practices, Security Guidelines, Security Standards, and Compliance and Assessments Processes	15
3.3	Grant Programs.....	16
3.4	Way Forward.....	19
3.5	Metrics.....	21
3.6	Transportation Sector Goals and Objectives	23
4	Program Management	24
5	Security Gaps	24

1 Executive Summary

The Highway Infrastructure and Motor Carrier Modal Annex to the Transportation Sector Specific Plan (TSSP) describes how transportation sector goals and objectives will be achieved to protect the highway transportation system. These assets include, but are not limited to, signature bridges, major tunnels, operations and management centers, trucks carrying hazardous materials (HAZMAT), other commercial freight vehicles, Motorcoaches, school buses, and key intermodal freight transfer facilities. All of these components help create what is referred to as the Highway Transportation System.

While the in-vehicle and highway facilities infrastructure optimizing the movement of people, services, and cargo through the Highway Transportation System are robust, some are essential in facilitating Federal and State services to maintain the health of the public, economic vitality, telecommunications, electricity, and other essential services. Even temporary debilitation of a bridge or tunnel could result in regional shutdowns, diversions, or costly repairs with potentially severe results. Security of the highway transportation system is a shared responsibility among Federal, state, and local governments and private stakeholders. Measures to secure the assets of the Highway Transportation System must be implemented in a way that balances cost, efficiency, and preservation of commerce in this Nation. The Highway Infrastructure and Motor Carrier Annex will require periodic updates to reflect current conditions, enhanced strategies, new programs, and Government Coordinating Council (GCC)/Sector Coordinating Council (SCC) scope of planning for the following year. Federal, State, local and tribal government agencies, along with private stakeholders, will lead the national effort to maintain the capability to move freely and facilitate interstate commerce in all conditions.

Vehicles that use the highways are potential targets and weapons that terrorists or criminals could use to attack critical infrastructure or other assets. The trucking industry is unique in that it is the only segment of the highway mode with complete intermodal supply chain relationships with aviation, maritime, mass transit, freight rail, and pipeline. The bus industry, similar to the trucking component, also operates with multi-modal interconnectivity daily, providing passenger and limited freight service on a national level. The diversity of these industries poses additional challenges to the effective integration of security into both large, complex operations and smaller owner-operator businesses.

To address these security issues, it is important the Federal Government continues to work effectively within the established government/industry partnership to implement a variety of security programs to enhance the security of domestic highway operations. Highway Infrastructure and Motor Carrier security is advanced by implementing layered security measures into transportation systems operations and management. Toward this end, the Department of Homeland Security (DHS), the U.S. Department of Transportation (DOT), State and local government entities, and the private sector security partners continue to be committed to improving the highway transportation system. Technology and human capability must keep pace with the increasingly sophisticated terrorist or criminal techniques that may be used to threaten the highway transportation system or its components.

2 Overview of Mode

Definition of Highway Transportation System: The physical components of the highway transportation system include the following basic features: infrastructure, vehicles, users, equipment, facilities, control/communication, and facilities. **Infrastructure**, the “fixed” part of the system, includes roads, bridges, tunnels, and terminals, where travelers and freight can enter and leave the system. Many **vehicle** types operate on the highway system, moving both people and freight. The **users** include the commercial vehicle and private passenger drivers, cargo shippers and receivers, passengers, and pedestrians. **Equipment** refers to the maintenance machinery that operates to facilitate transportation. **Facilities** refer to the terminals, warehouses, depots, and other transportation-related buildings. Finally, **control and communications** are methods for controlling vehicles, infrastructure, and entire transportation networks. These methods include both human and the application of technology to improve Highway Transportation System security and operations.

2.1 Vision of Mode

The vision of the highway mode is to lead the national effort to maintain the capability to move freely and facilitate commerce in all conditions, and to continuously set the standard for excellence in highway transportation security through our people, processes, and technology.

2.2 Description of Mode

The Nation’s highway transportation system is robust and interconnected, including 3.8 million miles of roadways, 582,000 bridges, and 54 tunnels over 500 meters in length. Significantly, the highway system supports 86 percent of all our citizens’ personal travel, moves 80 percent of the Nation’s freight (based on value), and serves as a key component in national defense mobility. Despite widespread redundancies, there are critical junctures with limited capacity for additional traffic. Freight volume is projected to double by 2020, stretching the Nation’s ability to manage limited capacity and growing security concerns.

Addressing potential threats to the highway system is particularly challenging because of the openness of the system. Vehicles and their operators move freely in the system, with almost no restrictions. Some bridge and tunnel elements are especially vulnerable because many structural elements are accessible and in isolated locations. State and local governments own most highways, although independent entities own some major, iconic structures. Protecting the highway transportation system is a shared responsibility between State and local transportation agencies and their sister agencies responsible for law enforcement. This reality is important when considering the potential costs of heightened security measures.

The trucking industry is made up of predominantly small private companies. Approximately 675,000 are interstate and 400,000 are intrastate companies. In addition to for-hire trucking, private truck operations are integral to other businesses operations, such as construction, agriculture, and the delivery of goods and services. Almost 8 million large trucks are registered in the U.S. While approximately 9.3 million truck drivers have Commercial Drivers Licenses (CDL), only 3.3 million are regarded as active. Vehicle configurations include tankers, dump trucks, intermodal containers, flat-beds, and specialty vehicles.

Trucks transport the majority of all the goods in the United States. These shipments include agricultural goods, hazardous materials, electronics, automotive, and other products essential to our economy. The trucking industry is unique in that it is the only segment of the highway mode with complete intermodal supply chain relationships with aviation, maritime, mass transit, freight rail, and pipeline. With widespread access to not only intermodal infrastructure, but also contact

with large numbers of people and goods, it is important that coordination between trucking operation and other modes include effective lines of communications and coordinated security measures to establish and maintain safe and secure transport of goods and people.

The motorcoach industry is comprised of approximately 3,600 motorcoach companies, operating 39,000 motorcoaches that carry close to 630 million passengers annually in the U.S. and Canada, traveling approximately 2.44 billion miles per year. The motorcoach industry, similar to the trucking component, also operates with multi-modal interconnectivity daily, providing passenger and limited freight service on a national level. Again, such open access requires coordinated safety and security efforts across modes.

The school transportation industry, which is comprised of approximately 460,000 school buses, is the largest public fleet of vehicles in the United States. Each day nearly 23.5 million minor students travel to approximately 14,000 public educational agencies nationwide. In the U.S., school buses travel 4 billion miles annually on daily fixed routes, as well as periodically conduct transportation to public venues.

2.3 GCC/SCC Structure and Process

Objective

The National Infrastructure Protection Plan (NIPP) calls for forming a GCC and SCC to provide a forum for coordination and information exchange.

The objective of the “Highway Infrastructure and Motor Carrier Modal GCC,” hereinafter referred to as the “Highway GCC,” is to coordinate highway and motor carrier security strategies and activities; to establish policies, guidelines and standards; and to develop program metrics and performance criteria for the mode. The Highway GCC fosters communication across government agency lines and between the government and private industry in support of the nation’s homeland security mission. It also functions as the counterpart to the private industry-led “Highway Infrastructure and Motor Carrier Modal Sector Coordinating Council” (Highway SCC) to review and develop security programs necessary to protect the Nation’s highway and motor carrier modes.

Scope of Activity: GCC

The Highway GCC will address highway infrastructure, commercial vehicle operations, and supporting facilities using the risk based methodology delineated in the NIPP and TSSP. The Highway GCC will accomplish this objective through the following activities:

Information-Sharing Mechanism

The Highway mode has the Highway Information Sharing Analysis Center (ISAC) and the Homeland Security Information Network (HSIN) as two mechanisms to share information with the highway industries.

Highway ISAC— The American Trucking Associations (ATA) operates the Highway Information Sharing and Analysis Center (ISAC) in partnership with the State and National trucking associations and conferences of the ATA Federation, numerous other national highway transportation organizations in the Highway Watch® Coalition in cooperation with DHS for the benefit of the entire Highway Transportation Sector.

The Highway ISAC disseminates information bulletins, alerts, and other security-related reports to stakeholders via e-mail. The ISAC works with both public and private stakeholders to collect, share, and analyze information that provides a security benefit for the highway mode.

The HSIN is intended to be a secure, single-source information-sharing Web-based network to assist in the two-way communication of security-related information. The Highway GCC has created a Web portal on HSIN. In addition, the Highway SCC will be creating their own Web portal on HSIN to allow private-sector stakeholders to engage in two-way communication with the public sector to share, review, discuss, and disseminate security information in an efficient and effective format.

Framework to Address Critical Issues

The Highway GCC and Highway SCC coordinate on projects involving policies that advance modal security. They may also meet to identify issues and provide recommendations or reports to the Transportation Sector GCC as necessary.

Membership

The Highway GCC membership consists of key Federal departments and agencies responsible for or involved in highway and motor carrier security. This membership may be expanded to include State/local officials with an interest in the highway and motor carrier mode.

The Highway GCC recognizes the integral relationship that it has with similar GCCs for other modes and will leverage its participation with these other councils to connect issues across modes at appropriate levels of Government and with private industry.

The Highway GCC will add permanent Federal department or agency members, as deemed necessary and appropriate. The Highway GCC will invite *ad hoc* members with special expertise from other departments, agencies or offices from time to time to meet expertise requirements necessary to fulfill its mission.

The following are member organizations of the Highway GCC:

- Transportation Security Administration
- Federal Motor Carrier Safety Administration
- Federal Highway Administration
- National Highway Traffic Safety Administration
- Pipeline and Hazardous Materials Safety Administration
- Department of Defense
- Department of Energy
- Nuclear Regulatory Commission
- DHS Customs and Border Protection
- DHS Office of Infrastructure Protection
- DHS Homeland Infrastructure Threat and Risk Analysis Center
- DHS National Preparedness Directorate
- DHS Office for State & Local Government Coordination
- American Association of State Highway Transportation Officials
- Commercial Vehicle Safety Alliance
- American Association of Motor Vehicle Administrators
- International Association of Chiefs of Police
- National Sheriffs' Association
- Federal Bureau of Investigation

Scope of Activity: SCC

Private sector owners and operators and representative associations of highway and motor carriers assets have formed a Highway Infrastructure and Motor Carrier Sector Coordinating Council (Highway SCC) to partner with senior government officials to collaborate and communicate on security initiatives designed to enhance the protection of the transportation sector's critical infrastructure and key resources. The Highway SCC is an industry advisory body that, as appropriate, will coordinate the private industry perspective on highway and motor carrier security policy, practices, and standards that affect the transportation sector.

The Highway SCC will operate in a similar manner to the GCC described above. It includes members from the motorcoach, school bus, the trucking industry, and related associations. Many of the members are either an association representative or an employee for a private company in one of the highway transportation industries.

The objectives of the SCC are to:

- Facilitate intra-sector communications, set processes for information sharing, and facilitate priority setting on sector strategy and planning; policies and procedures; threat communication and analysis; as well as sector protection, response and recovery planning and activities
- Serve as an interface with DHS, and other Federal and State agencies on homeland security matters
- Facilitate communications, plans, and activities with other relevant infrastructure sectors, government entities, and others necessary to further secure the Nation's highway and motor carrier critical infrastructure assets
- Communicate the sector's needs and requests for resources to the Highway GCC.

The following are member organizations of the Highway SCC:

- American Bus Association
- American Chemistry Council
- American Petroleum Institute
- American Road and Transportation Builders Association
- American Trucking Associations
- Border Trade Alliance
- Con-Way, Inc.
- Detroit-Windsor Truck Ferry
- Institute of Makers of Explosives
- Intelligent Transportation Society of America
- Intermodal Association of North America
- International Bridge Tunnel and Turnpike Association
- Kenan Advantage Group
- Laidlaw Education Services
- Mid-States Express, Inc.
- National Association of Small Trucking
- National Association of Truck Stop Operators
- National Industrial Transportation League
- National School Transportation Association
- National Tank Truck Carriers, Inc.
- Owner-Operator Independent Drivers Association

- Taxicab, Limousine and Paratransit Association
- The BusBank
- The National Academies, Transportation Research Board
- Tri-State Motor Transit Company
- Truck Manufacturers Association
- Truck Rental and Leasing Association
- United Motorcoach Association

3 Implementation Plan

3.1 Priorities and Programs

3.1.1 Priorities

The mission of the transportation systems sector is to continuously improve the risk posture of the national transportation system using a risk management framework. The TSSP identifies a number of goals for enhancing security in the transportation sector.

Goals:

1. Prevent and deter acts of terrorism using or against the transportation system
2. Enhance resilience of the transportation system
3. Improve the cost-effective use of resources for transportation security

The public sector has developed a number of critical voluntary and mandatory programs that incorporate elements to target, assess risk, and secure the highway transportation system. Many of these efforts encourage private-sector initiatives in security and increase the government's visibility in the highway transportation system without disrupting the movement of cargo or people. Many programs of the Federal Government are currently focused on security awareness training, technology, and screening programs. These programs seek to develop common security practices to mitigate security risks. Some government-led efforts are outlined below.

The sector has identified ways to achieve these goals, including: the standardization of risk assessment and risk mitigation approaches; the establishment of performance-based security guidelines through collaboration with stakeholders; the integration of security measures into the design of the Nation's transportation network; the use of existing security grant programs; development and adoption of security technology; enhancement of driver threat assessments and credentialing; enhancement of existing HAZMAT security requirements; and the enhancement of owner-operator and law enforcement awareness and training. A description of key priorities and program details follows. The programs described below are designed to implement more than one goal or objective although discussed here under their primary objective. For a comprehensive list of programs and their corresponding goals, see Figure D3-1.

3.1.2 Sector Goals and Objectives

Goal 1: Prevent and deter acts of terrorism using or against the transportation system

Objectives

Implement flexible, layered, and effective security programs using risk management principles. The highway sector will develop and implement layered security programs using risk management principles (discussed in Chapters 3 through 7 of the TSSP). Sustained focus on the following risk-based priorities for highway infrastructure and the motor carrier industry will reduce vulnerability and minimize the consequences of a terrorist attack, while also improving the efficiencies of this important and complex transportation network.

- **Standardize Risk Assessment and Risk Mitigation Approaches.** Coordinated communication between the public and private sectors will assist in making informed decisions on the use of limited resources in areas of greatest risk. The Federal

Government will continue to partner with the private sector to improve the risk assessment system that all highway stakeholders within similar industry disciplines can use to identify risk, based on threat, vulnerability, and consequence. This task involves identifying each major segment of the Highway Transportation System: structural, conveyances, systems and personnel and the specific aspects, vulnerabilities and mitigation strategies common to all and unique to each. Federal partners will work to develop assessment and mitigation solutions for each. TSA, the Federal Motor Carrier Safety Administration (FMCSA), and the Federal Highway Administration (FHWA) are currently working to combine their individual risk assessment and risk mitigation tools into one document that will reduce redundancy, increase efficiencies, and minimize impact on private stakeholders.

- **Corporate Security Review (CSR) Program.** CSRs are conducted with organizations engaged in transportation by motor vehicle and those that maintain or operate key physical assets within the highway transportation community. They serve to evaluate and collect physical and operational preparedness information, critical assets and key point-of-contact lists, review emergency procedures and domain awareness training, and provide an opportunity to share industry best practices.
- **Security Action Items (SAI).** Consistent with Executive Order 13416, TSA is drafting Security Action Items (SAI) that are voluntary practices designed to improve security for trucks carrying security-sensitive HAZMAT, motorcoach and school buses, and highway infrastructure. These SAIs are being coordinated with DOT's FMCSA and FHWA. Once the SAIs are completed, the HMC SCC will solicit and obtain industry review and input on the SAIs prior to issuance. SAIs, though voluntary, will allow TSA to communicate and share formally with applicable stakeholders those security actions identified as key elements within an effective and layered approach to transportation security. Many of the applicable stakeholders are currently employing some of these security actions as evidenced by the results of CSR HMC conducted.

The Federal Government will work with highway stakeholders to identify and establish measurable security action items. Performance-based standards provide highway asset/system owners and operators the flexibility to tailor approaches to each facility's unique risks and configurations; they could include standards for enhancing physical and cyber-security, including surveillance detection, escalating perimeter/access controls for heightened alert status, and structural hardening. The Federal Government will also work with the private sector to develop a catalog of highway-specific protective measures that correspond with the Homeland Security Advisory System (HSAS) levels, and apply existing best practices. Further, FHWA and TSA are working with State DOTs to incorporate security programs as part of their "all hazards" approach to emergency planning, preparedness and response.

- **FHWA Security Self-Assessment Tool.** The FHWA's Security Self-Assessment Tool assist their field offices work with their State DOT counterparts to (a) assess the current state of highway transportation security and (b) identify potential areas for improvement. This tool consists of a discussion paper entitled *Attributes of an Effective State Highway Asset Security Program* and a checklist to use in assessing the current state of practice. The intent is to review State security processes and procedures on a 2-year cycle to ensure that State programs keep abreast of changes in security conditions, identifying program areas for improvement and monitoring progress.

Increase vigilance of travelers and transportation workers. By having an active role in identifying and reporting suspicious activity, the traveling public and transportation workers can serve as force multipliers to Federal, State, and local law enforcement efforts.

- **Enhance Owner-Operator and Law Enforcement Awareness and Training.** The Federal Government will work closely with industry stakeholders, and State, local, and tribal governments to enhance truck and Motorcoach awareness and training. Existing Federal site visit programs will be coordinated to enhance security awareness and training, and provide technical and threat information. This effort will build upon existing complementary DHS and DOT efforts. The Federal Government will also provide assistance to the bus and Motorcoach industry to develop and implement security plans and security training for employees. Enhancing programs that support law enforcement agencies, such as DOT's "Trucks 'n Terrorism" training and courses DHS's Federal Law Enforcement Training Center offer, will raise awareness of indicators of suspicious activities involving commercial motor vehicles.
- **Consolidate Driver Threat Assessments and Credentialing Programs.** Congress passed the "REAL ID Act" in 2005. DHS issued a Notice of Proposed Rulemaking in March 2007 which proposes to significantly enhance the security of the issuance of state driver's licenses.

DHS requires all individuals who receive, renew, or transfer a HAZMAT endorsement for a commercial drivers license to successfully complete a rigorous background check. Efforts are also underway to evaluate the need for improvements to the risk-based approach for background checks for drivers transporting certain types of HAZMAT

As employee and "insider" vetting programs proliferate throughout the transportation industry, DHS, DOT, and the stakeholder community have recognized the inefficiency and potential security gaps that can be created by disparate programs that are not coordinated in purpose or distribution. Because of this concern, DHS is intensifying its effort to harmonize vetting programs, background checks, and disqualification standards across modes and purposes.

DHS is also working on the Transportation Worker Identification Credential (TWIC) program and will be able to harmonize background check programs. TWIC will focus on those individuals requiring unescorted access to secure areas of Maritime Transportation Security Act (MTSA) regulated facilities, vessels and Outer Continental Shelf facilities (OCS). Under the TWIC program, drivers who have already successfully undergone a security threat assessment to obtain an HME will not be required to obtain a new security threat assessment and will receive a TWIC card for a discounted fee.

- **Security Plans and Training.** DOT regulations (49CFR172), effective September 25, 2003, require shippers and carriers of certain HAZMAT deemed to present a security

risk in transportation to develop and implement security plans. All shippers and carriers must also ensure that employee training includes a security awareness component. The security plan must be based on an assessment of possible transportation security risks and appropriate measures to address the assessed risks. Specific measures the plan puts into place may vary commensurate with the level of threat at a particular time. At a minimum, a security plan must address personnel security, unauthorized access, and en route security. The regulations permit a company to implement a security plan tailored to its specific circumstances and operations. DOT modal administrations—such as FMCSA—review security plans as part of ongoing HME programs. Although regulations do not require motor carriers to obtain government approval of security plans, enforcement personnel take advantage of scheduled safety inspections (which include determining whether companies have a security plan) to review security plans and provide informal suggestions for improvement. DOT is evaluating security plan regulations. It is evaluating an industry petition that certain HAZMAT that pose little or no security risk be for removed from the list requiring security plans. Other possible changes or clarifications include designating a high-level corporate focal point for HAZMAT security plans, specifying that security plans must be site-based rather than corporatewide, and adding coverage on government access and review.

Enhance information and intelligence sharing among Highway Transportation System Sector partners. The development and maintenance of relationships and improved technology can provide Federal, State, local, tribal, private sector, and international transportation security partners with a platform to share and exchange security information such as threats, best practices, lessons learned, or other experiences to improve transportation security.

- **FHWA Security and Emergency Management Professional Capacity Building Program.** FHWA, in partnership AASHTO, has developed a strategic plan for security training of State and local transportation officials. This strategic plan for professional capacity building is designed to provide state DOTs with trusted, reliable, and reasonably comprehensive sources of information and assistance to meet their obligations for securing the Nation's transportation network and meeting their emergency response needs. Highlights of the program kick-off in FY 2006 included a pooled fund solicitation inviting States to contribute funds to support the development and delivery of training, technical assistance and peer support for risk assessment principles and methods, emergency transportation operation, and evacuation planning. In addition, FHWA and the TSA initiated a series of regional workshops that brought together security and emergency transportation operations specialists from all states to share best practices and ideas to meet their operational needs.

Goal 2: Enhance resilience of the U.S. transportation system

Objectives

Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability.

- **Integrate Security Measures into the Design of the Nation's Transportation Network.** Improved methods for cost-effective access control and surveillance/detection will decrease the risk of attack. Design/analysis methods and materials for highway structural hardening, improved standoff distance and barrier designs, and enhanced

response/recovery will aid in mitigating risk. Because of the complexity of interacting modes, comprehensive analyses, innovative integrated measures, and tailored training, specialized technology will be required to support intermodal facilities. FHWA currently has a number of programs and resources available to assist highway infrastructure stakeholders recognize and incorporate security measures into the design and construction of highways, bridges, and tunnels.

- **FHWA-Supported Security Research and Development Program.** The FHWA has dedicated a portion of its structural R&D program to developing new techniques for enhancing the security and resiliency of highway-related structures. In 2006, FHWA published a report, titled *Multiyear Plan for Bridge and Tunnel Security Research, Development, and Deployment (9FHWA-HRT-06-072)*, which can be accessed on the Web at www.tfhrc.gov/structur/pubs/06072/index.htm. It presents a strategic plan to secure the Nation's highway infrastructure and is based on input from experts in bridge engineering and other stakeholders. The FHWA and DHS's Office of Science and Technology are exploring a cooperative relationship in delivering research based on this strategic plan. FHWA is also continuing its cooperative research with the Army Corps of Engineers to develop options for retrofitting existing bridges. Promising advances have been made to protect some of the Nation's most critical bridge components from terrorist threats through this FHWA-led pooled fund study. End products will include retrofit options and design guidance on blast-resistant bridge elements for American Association of State Highway and Transportation Officials' (AASHTO) consideration.
- **Explore the Use of Existing Grant Programs to Support Critical Highway Infrastructure Security Improvements.** Investments in hardening highway infrastructure can improve highway safety and security. Financial resources to support highway infrastructure hardening are limited, however, and resource decisions can be challenging. The Federal Government will work with State, local, and tribal governments to coordinate specific grants programs with other related grant programs to leverage the benefits from limited resources.

Enhance the capacity for rapid and flexible response and recovery to all-hazards events.

- **FMCSA Hazardous Materials Safety Permit Program.** This program was established on January 1, 2005. Congress directed FMCSA to implement the HAZMAT permit program to produce a safe and secure environment to transport certain types of HAZMAT. Within this program lies a requirement for certain motor carriers to maintain a security program and establish a system of communication to enable commercial motor vehicle drivers to contact motor carriers during the course of transportation of these HAZMAT. This safety and security program use the security contact reviews (SCR) program to collect specific security information on the motor carrier's ability to secure certain type of HAZMAT.

Goal 3: Improve the cost effective use of resources for transportation security.

Objectives

Ensure robust sector participation in the development and implementation of public sector programs for U.S. highway transportation sector.

- **Highway Infrastructure and Motor Carrier GCC and SCC:** The Federal Government uses the Highway GCC and Highway SCC for partnership efforts that provide consensus recommendations regarding security standards and processes. The Federal Government will continue to maintain these partnerships to ensure robust participation from relevant partners in highway transportation sector security.
- **Truck Security Program (TSP).** The Trucking Security (Grant) Program is to sustain the Highway Watch® Program to enhance homeland security through increased vigilance and awareness on our Nation's highways. The FY 2006 TSP awarded \$4,801,500 (out of a total appropriation of \$5M) directly to ATA. TSP seeks to assist all professionals and operating entities throughout the entire highway sector in obtaining training on security awareness, reporting suspicious incidents, and information analysis.
- **Infrastructure Protection Program: Intercity Bus Security Grant Program (IBSGP).** The mission of the IBSGP is to, through the distribution of grant money to eligible stakeholders, create a sustainable plan for protecting intercity bus systems and the traveling public from terrorism, especially from explosives and non-conventional threats that would cause major loss of life and severe disruption. The fiscal year (FY) 2006 IBSGP awarded \$9.5 million. TSA is providing subject matter expertise for evaluating grant applications.

Ensure coordination and enhance risk-base prioritization of research, development, testing, and evaluation efforts.

- **Research the Viable Use of Current and Emerging Security Technologies.** The Federal Government will continue to review the potential use of technology standards for commercial vehicles carrying high-risk cargoes [e.g., toxic inhalation hazard (TIH), explosives]. A recent DOT study showed that some technologies are dual-use, providing improved security benefits, improved safety benefits, and business efficiencies. These technologies include electronic tracking, panic alerts, driver identification systems, and satellite-based mobile communications tracking. Significant, further research and development (R&D) of these systems is necessary to demonstrate their effectiveness and inherent security benefit before any reliable strategy and policy can be developed.

3.1.2 Public-Private Partnership Programs

As the owners and operators of transportation assets, the private sector has made contributions to the achieving the goals of the transportation sector. Private industry has adopted various security measures that supplement government-led regulations and programs. Industry practices and guidelines focus on achieving security through countermeasures associated with employees/people, information, technology, and cyber/physical infrastructure.

The following three programs are partnerships between private industry and the public sector designed to continually enhance the risk posture of the U.S. highway transportation sector:

- **Intercity Bus Security Grant Program (IBSGP)** .
- **Truck Security Grant Program**
- **National Cooperative Highway Research Program Project 20-59.** AASHTO, through its Special Committee on Transportation Security, directs a security and

emergency operations R&D program funded through the National Cooperative Highway Research Program (NCHRP), administered by the Transportation Research Board at the National Academy of Science. Funding for NCHRP efforts is made available each year from the Federal-aid Highway Program and is allocated to the various R&D efforts based on problem statements State DOTs and the FHWA submit. The NCHRP 20-59 Project has funded the development of a risk management guide, an emergency transportation operations guide, a guide on managing sensitive information, guidance on continuity of operations planning, as well as a number of other more focused reports on special interest topics. More detailed information can be found at <http://www4.trb.crp.nsf/All+Projects/NCHRP+20-59> . The AASHTO Subcommittee on Bridges and Structures also has a committee on bridge security, which provides guidance and support on research needs and for developing research problem statements for implementation through the regular NCHRP program. The committee's role is to ensure that relevant research is conducted that will lead to specific development for design and construction of bridges and structures for security. The committee is also developing a strategic research program for the security of bridges and structures.

- **TSA Missouri Pilot Program.** This pilot program is intended to conduct a Corporate Security Review of trucking and Motorcoach companies using state inspectors. It is the result of a partnership between the Commercial Vehicle Safety Alliance (CVSA), the State of Missouri DOT, and TSA. TSA trained 44 Missouri DOT officers to conduct CSRs while they are also conducting safety inspections for the FMCSA.

Through this program TSA expects to collect additional security data while testing the feasibility of using roadside enforcement officers to examine security issues. It will also assist the HMC in collecting and assessing best security practices and providing targeted security assistance. The pilot program began in March 2006 and is expected to run until June 30, 2007. TSA will evaluate the results of this program and determine feasibility and effectiveness of using state inspectors for CSRs.

3.1.2 Other Initiatives and Pilot Programs

Building on these previous efforts, all sector security partners will continue working together to develop an overarching portfolio of risk-based security programs and countermeasure to improve the highway transportation sector's risk profile and achieve the mode's goals and objectives. The following describes current initiatives and pilot programs.

- **TSA HAZMAT Driver Security Threat Assessments.** Section 1012 of the USA PATRIOT Act, requires all commercial drivers seeking to apply for, renew, or transfer an HME on their state-issued CDL must undergo a "security threat assessment" to determine whether or not the individual poses a security risk. Individuals may be disqualified from holding an HME based on the assessment, which is comprised of an FBI fingerprint-based criminal history records check, an intelligence check, and immigration status verification. Drivers determined to be a security threat are prevented from receiving HMEs on their CDLs.
- **Truck Tracking Security Pilots.** The ability to track trucks, especially those carrying certain HAZMAT, has potential security benefits. FMCSA has conducted a tracking pilot and TSA is in the midst of conducting one. FMCSA conducted a 2-year national field operational study of existing technologies offering enhanced solutions

to the security of motor carrier shipments of HAZMAT was completed in December 2004. The test evaluated the costs, benefits, and operational processes required for wireless communications systems, including global positioning satellite (GPS) tracking and other technologies. The tested technologies performed well under operational conditions and showed promise for significantly reducing security vulnerabilities. TSA is testing near real-time tracking and identification systems, theft detection and alert systems, motor vehicle disabling systems, and systems to prevent unauthorized operation of trucks and unauthorized access to their cargos. As a result of this pilot, TSA will be able to evaluate such factors as costs and benefits of the system; ability to collect, display and store information on shipments of high-risk materials by motor vehicle and/or trailer throughout the supply chain; and the capability of the system to resist accidental or unauthorized disabling.

- **Hazardous Materials Research Involving Security Initiatives.** DOT and DHS have current and ongoing R&D projects that will directly impact securing highway transportation facilities, conveyances, and critical infrastructures. Both Departments will work closely together to coordinate these projects. FMCSA will be working on congressionally mandated projects and agency-funded projects. One is a continuation of the Hazardous Materials Transportation safety and security testing, including conducting research on the cost/benefit analysis of using truck disabling technologies. FMCSA will also perform testing and evaluation of mobile and stationary radiation detection devices (RDD) used on trucks. They will also evaluate current routing activities and provide a comprehensive analysis of the safety and security concerns related to HAZMAT routing in the United States. Both departments are also evaluating various commercial software packages designed to assist first responders when responding to HAZMAT and other transportation incidents.
- **FHWA Statewide and Project-specific Vulnerability Assessments.** FHWA has trained a cadre of engineers to assess bridges and tunnels for vulnerability to terrorist threats. The engineering assessment team conducts assessments, at the request of the owners, for project-level, facility-level, and for statewide critical structures. The objective is to guide facility owners and operators to identify vulnerable components and measures to reduce vulnerability.
- **FHWA Bridge and Tunnel Vulnerability Workshops.** FHWA teamed with the U.S. Army Corps of Engineers (COE) to develop training for bridge and tunnel engineers to protect the physical security of critical transportation assets. The workshops address terrorist threats to bridges and tunnels, vulnerabilities to these threats, and potential mitigations to reduce risk.
- **FMCSA Sensitive Security Visit (SSV) and Security Contact Review (SCR).** FMCSA conducts security sensitive visits (SSV) and SCRs as part of its regular compliance reviews of HAZMAT carriers. SSVs are educational security discussions covering best practices. They are conducted with HAZMAT motor carriers that do not require a security plan. SCRs are comprehensive reviews of security plans and their implementation that are conducted on all HAZMAT motor carriers that transport placardable amounts of HAZMAT.
- **TSA School Transportation Security Awareness (STSA).** Twenty-five million children ride 500,000 school buses daily in the United States. TSA Highway and

- Motor Carrier Division is working with a contractor to develop a school transportation security awareness training program that promotes a better understanding among school transportation personnel of the vulnerabilities of their systems and appropriate mitigation strategies to address those vulnerabilities. The contractor will also create a Facility Security Assessment Program for school entities to use in developing their site-specific security programs. STSA will provide approximately 140 minutes of online, or on-site training to small groups of personnel in localities that operate school bus transportation—school bus drivers in particular. The training program will contain significant graphic content and use up-to-date interactive teaching methods. The school bus community consists of three major associations: The National School Transportation Association (NSTA), National Pupil Transportation Association (NAPT), and the National Association of State Directors of Pupil Transportation Services (NASDPTS). These associations are collaborating with the contractor/vendor Consolidated Safety Services (CSS) in this security initiative.
- **Evaluate Hazmat Security Requirements.** The Federal Government is evaluating the need to harmonize existing security and safety regulations for hazmat transport. As appropriate, the Federal Government will solicit and incorporate, industry stakeholder input to evaluate, revise, and where necessary, enhance existing DOT and DHS HAZMAT security regulatory requirements in keeping with current security threats, research, and technologies. Appropriate coordination will be considered for an ongoing effort to evaluate potential subsets of the DOT safety-driven HAZMAT list.

3.1.3 Implementation

The most effective security programs will involve cost-effective security planning, risk assessment and layered mitigation strategy development. They will also include multifaceted training and technical assistance to the transportation industry supported by R&D efforts to promote and advance new security technologies.

TSA and DOT's FHWA and FMCSA are dedicated to improving the security posture of the Nation's highways. All three have developed and implemented initiatives, identified gaps or evaluated vulnerabilities, and are working together and with their industry partners to implement effective mitigation strategies.

3.2 Effective Practices, Security Guidelines, Security Standards, and Compliance and Assessments Processes

Executive Order 13416 requires the identification of existing security guidelines and security requirements for each surface transportation mode. The following describes current regulations and any proposed regulatory action for highway infrastructure and motor carrier security. The conveyance of HAZMAT poses the greatest threat to the highway infrastructure and motor carrier mode. Current regulatory action focuses on mitigation of this threat.

The U.S. DOT established a rule in 2003, HM232 (49 CFR 172.800) that requires shippers and carriers of certain highly hazardous materials to develop and implement security plans. In addition, all shippers and carriers of hazardous materials must assure that their employee training includes a security component.

The TSA passed a rule, 49 CFR Parts 1570 and 1572 that establishes security threat assessment standards for determining whether an individual poses a security threat warranting denial of a HME for a CDL. TSA will determine that an individual poses a security threat if he or

she: (1) Is an alien (unless he or she is a lawful permanent resident) or a U.S. citizen who has renounced his or her U.S. citizenship; (2) is wanted or under indictment for certain felonies; (3) has a conviction in military or civilian court for certain felonies; (4) has been adjudicated as a mental defective or committed to a mental institution; or (5) is considered to pose a security threat based on a review of pertinent databases. The rule establishes conditions under which an individual who has been determined to be a security risk may appeal the determination, and procedures TSA will follow when considering an appeal. The rule also provides a waiver process for those individuals who otherwise cannot obtain a HME because they have a conviction for a disqualifying felony, or were adjudicated as a mental defective or committed to a mental institution.

Consistent with Executive Order 13416, TSA is drafting Security Action Items (SAI) that are voluntary practices designed to improve security for trucks carrying security-sensitive HAZMAT, motorcoach and school buses, and highway infrastructure. These SAIs are being coordinated with DOT's FMCSA and FHWA. Once the SAIs are completed, the HMC SCC will solicit and obtain industry review and input on the SAIs prior to issuance. SAIs, though voluntary, will allow TSA to communicate and share formally with applicable stakeholders those security actions identified as key elements within an effective and layered approach to transportation security. Many of the applicable stakeholders are currently employing some of these security actions as evidenced by the results of CSR HMC conducted (see separate topic paper on CSRs).

3.3 Grant Programs

Since FY 2003, there have been non-recurring security grant funds for both intercity/charter bus operations and trucks. The security grant money appropriated for trucks to supports the ATA's Highway Watch® program described in more detail below. DHS has administered the distribution of these grant funds.

Figure 1: Grant Programs

Program	Program Description	Funding Level FY 06	Funding Level FY 07
Intercity Bus Security Grants	See 3.1 Program # 15	\$10M	\$11.64M
Truck Security Grants	See 3.1 Program # 16	\$5M	\$11.64 M

Intercity Bus Security Grant Program

As a component of the DHS Infrastructure Protection Program (IPP), the IBSGP seeks to assist owners and operators of fixed route intercity and charter bus services in obtaining the resources required to support the national priorities. Current priorities focus on enhanced planning, passenger and baggage screening programs, facility security enhancements, vehicle and driver protection, as well as training and exercises, the FY 2006 IBSGP directly addresses the DHS National Response Plan and Targeted Capabilities priorities:

1. Expanded regional collaboration
2. Implementing the National Incident Management System (NIMS) and the National Response Plan (NRP)
3. Implementing the interim NIPP

Figure 2 Program and Goals/Objectives Matrix

The chart shows the relationship of each project to the transportation sector goals and objectives

		Transportation Sector Goals and Objectives												
		Goal 1 – Prevent and deter acts of terrorism using or against the U.S. transportation system	Goal 1A: Implement flexible, layered and unpredictable security programs using risk management principles	Goal 1B: Increase vigilance of travelers and transportation workers	Goal 1C: Enhance information and intelligence sharing among transportation security partners	Goal 2 – Enhance resiliency of the U.S. transportation system	Goal 2A: Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability	Goal 2B: Ensure the capacity for rapid and flexible response and recovery to all-hazards events	Goal 2C: Implement risk-based measures to improve the redundancy and robustness of key nodes, links, and flows	Goal 3 - Improve the cost-effective use of resources for transportation security	Goal 3A: Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria	Goal 3B: Ensure robust sector participation as a partner in developing and implementing public sector programs for Critical Infrastructure/Key Resource protection	Goal 3C: Improve coordination and risk-based prioritization of Transportation Sector Security Research, Development, Test and Evaluation efforts.	Goal 3D: Align risk analysis methodologies with RAMCAP (Risk Analysis and Management for Critical Asset Protection) criteria outlined in the National Infrastructure Protection Plan.
HIGHWAY AND MOTOR CARRIER PROGRAMS	1. FHWA Bridge and Tunnel Vulnerability Workshops		✓	✓			✓	✓	✓					
	2. FHWA Statewide and Project Specific Vulnerability Assessments		✓	✓			✓	✓	✓		✓			
	3. TSA Security Action Items (SAI)		✓	✓	✓			✓	✓		✓	✓	✓	
	4. TSA Intercity Bus Security Grant Program (IBSGP)										✓			
	5. TSA Truck Security Grant Program		✓	✓							✓			
	6. FHWA-Supported Security Research and Development Program		✓					✓						
	7. National Cooperative Highway Research Program Project 20-59		✓					✓				✓		✓
	8. FMCSA & TSA Truck Tracking Security Pilots		✓					✓			✓		✓	
	9. Hazardous Materials Research Involving Security Initiatives		✓								✓			
	10. TSA HAZMAT Driver Background Rulemaking		✓											
	11. FMCSA Hazardous Materials Safety Permit Program		✓					✓						
	12. Security Plans and Training		✓	✓				✓						
	13. FHWA Security Self-Assessment Tool		✓					✓	✓		✓			

The chart shows the relationship of each project to the transportation sector goals and objectives

		Transportation Sector Goals and Objectives												
		Goal 1 – Prevent and deter acts of terrorism using or against the U.S. transportation system	Goal 1A: Implement flexible, layered and unpredictable security programs using risk management principles	Goal 1B: Increase vigilance of travelers and transportation workers	Goal 1C: Enhance information and intelligence sharing among transportation security partners	Goal 2 – Enhance resiliency of the U.S. transportation system	Goal 2A: Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability	Goal 2B: Ensure the capacity for rapid and flexible response and recovery to all-hazards events	Goal 2C: Implement risk-based measures to improve the redundancy and robustness of key nodes, links, and flows	Goal 3 – Improve the cost-effective use of resources for transportation security	Goal 3A: Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria	Goal 3B: Ensure robust sector participation as a partner in developing and implementing public sector programs for Critical Infrastructure/Key Resource protection	Goal 3C: Improve coordination and risk-based prioritization of Transportation Sector Security Research, Development, Test and Evaluation efforts.	Goal 3D: Align risk analysis methodologies with RAMCAP (Risk Analysis and Management for Critical Asset Protection) criteria outlined in the National Infrastructure Protection Plan.
14.	TSA Corporate Security Review (CSR)			✓							✓			
15.	TSA Missouri Pilot										✓		✓	
16.	FMCSA Sensitive Security Visit (SSV) and Security Contact Review (SCR)			✓			✓				✓			
17.	FHWA Security and Emergency Management Professional Capacity Building Program			✓										
18.	TSA School Transportation Security Awareness (STSA)		✓	✓							✓		✓	

4. Strengthening information sharing and collaboration capabilities
5. Strengthening interoperable communications
6. Chemical, biological, radiological, nuclear and explosive (CBRNE) detection and response capabilities.

In addition, the FY 2006 IBSGP also supports strengthening emergency operations planning and citizen protection capabilities, and assisting in addressing security priorities specific to the intercity bus industry. When developing project proposals, specific attention was paid to preventing, detecting, and responding to incidents involving improvised explosive devices (IED).

Truck Security

DHS has also distributed grant money to the commercial motor carrier stakeholder community to improve security awareness and suspicious activity reporting. These funds have been directed to the Highway Watch® program, which the ATA administers. With these grant funds, commercial vehicle operators, and other highway professionals have implemented domain awareness programs to meet identified security vulnerabilities. These programs include training in awareness and self-protection training for truckers, making significant improvements to first responder communications, and creating security incident reporting and analysis channels.

3.4 Way Forward

The Highway GCC will continue to engage the private sector to explore advances in security and to develop programs that are mutually acceptable and will result in increases in security.

There are significant challenges confronting all stakeholders, private and public, directly involved in securing the highway mode of transport. These challenges will have to be overcome before significant and meaningful security improvements can be realized. Before identifying challenges specifically, it is worth mentioning again the complexity and diversity of the highway mode. It is vast and involves literally tens of thousands of private and public stakeholders. Key components of the highway mode include: (1) trucking, (2) motorcoach, charter, and school buses, and (3) highway infrastructure, specifically highways, bridges and tunnels. The first two represent roughly 60 thousand stakeholders, mostly trucking and charter bus operators. DHS Secretary Chertoff frequently reminds the American public "...that while no government can protect every person against every threat in every place at every moment..." DHS has made and continues to make significant progress to prevent another catastrophic attack against our nation.

A continuing challenge will be aligning resources and responsibilities. At the Federal level, the key agencies that have a security focus are the DHS's TSA and the DOT's FMCSA, FHWA, and Pipeline and Hazardous Material Safety Administration (PHMSA), and the FBI's National Joint Terrorism Task Force (NJTTF). Each agency will need to administratively balance operational needs and requirements to ensure they meet the commitments of the NIPP and TSSP. State and local governments will have similar challenges. Additionally, private operators continually try to balance operational demands and costs and maintain an effective level of security. We must ensure, through a risk-based approach, to maximize the security effectiveness of the resources available. Program dollars to support security enhancements and security grant dollars for mitigating identified vulnerabilities outlined in security plans.

Another challenge is synchronizing the Federal approach to establishing regulations, security guidelines, and/or requirements for the highway mode. Currently, certain DOT agencies, specifically PHMSA and FMCSA, have issued security rules addressing the transportation of HAZMAT and the requirement for security plans. TSA, as stated above in section 3.2, is in the process of developing voluntary security guidelines entitled 'Security Action Items'. These

guidelines, prior to distribution, will be developed in concert with DOT and other Federal and industry stakeholders. The coordination process with Federal, State, local, tribal and private stakeholders should become more routine and streamlined as all become comfortable utilizing the GCC and SCC framework addressed earlier in this plan. This coordination will be very important to ensure the issuance of future guidelines, standards, and any other requirements are done effectively and systematically.

Related to the challenge of coordinating the issuance of guidelines, requirements, standards, and regulations is the need to ensure compliance. The compliance challenge is directly related to the diversity and sheer number of stakeholders mentioned in the first paragraph of this section. The effectiveness of any requirement is only as good as the ability to periodically and systematically ensure that all issued requirements have been implemented and are being followed. It will take creative leveraging of resources to develop and implement an effective compliance program.

One of the key security threats in the highway mode is the potential deliberate misuse of HAZMAT transported on the highway, especially those HAZMAT deemed to be particularly dangerous and attractive to terrorists. One of the priorities identified in this plan is to continue to evaluate existing HAZMAT security requirements. The need for the following actions will be further evaluated:

HAZMAT Tracking

Upon completion of the TSA truck tracking pilot in spring 2007, further evaluation will be made regard requiring trucks transporting some HAZMAT such as explosives, TIH, and radioactive materials (RAM) be equipped with satellite or terrestrial tracking transceivers enhanced with GPS and be monitored while in-transit by a government-centralized tracking site. This could provide many benefits, such as near real-time receipt by the tracking site of emergency alerts generated by trucks, near-immediate tracking site notification to police that an emergency alert had been received, automated identification of in-transit truck delays by the tracking site, ability of the tracking site to quickly identify and work with industry to have trucks moving toward geographic areas with increased security threat levels diverted, and ability of TSA to quickly obtain shipment movement record data archived by the tracking site for analysis of the type shipments moving, when, where, in what quantity, and via what routes. The latter could be a valuable tool for use in conducting analysis to support optimum allocation of scarce security resources. This would constitute a logically progressive use of the tracking technology already in use for the most part by motor carriers transporting the type HAZMAT noted above.

HAZMAT Shipments Movements Directly To Destination

One of the key means to ensure the secure movement of some HAZMAT shipments such as explosives, TIH, and RAM is to minimize the transit time and resultant public exposure. A specific requirement to this end may be considered for these type shipments. If implemented, this would also have the effect of minimizing the current perceived need for secure and safe areas for trucks transporting these types of HAZMAT to temporarily stop at while in-transit. The current practice of permitting stops may actually present more of a security risk due to public knowledge of the sites, and the aggregation of HAZMAT most susceptible to being weaponized by hostile elements.

HAZMAT Shipments Avoiding Standard Routes When Transiting Identified Target Areas

Consideration could be given to requiring some shipments of HAZMAT such as explosives, TIH and RAM avoid using standard routes when transiting areas identified as target areas for hostile elements. This could maximize unpredictability and thereby increase the difficulty for those

elements to conduct attack planning. In order to meet this requirement, some shipments might have to travel a longer distance through areas with potentially smaller roads and less experienced emergency response personnel. This could present a higher risk of an accident. However, the potential increased safety issue may be deemed acceptable to mitigate the security risk.

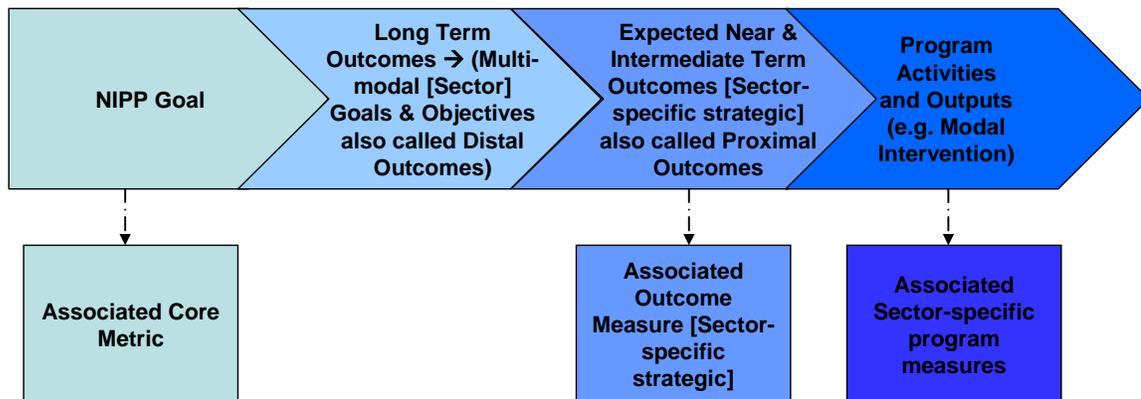
3.5 Metrics

General. To evaluate the collective impact of the transportation sector’s efforts to mitigate risks to the transportation infrastructure and to increase the resilience of the transportation system through information-sharing mechanisms, measures of effectiveness will be developed and monitored. Metrics that are developed will supply the data either to affirm that TSSP goals are being met or to show what corrective actions are required. This section overviews the plan to implement a TSSP measurement program. To be effective, the measurement program will require the cooperation of all modal GCCs and SCCs to provide accurate responses to the metrics being used to measure sector risk posture, SSP effectiveness in the sector, and security program effectiveness.

Measurement Joint Working Group. A Measurement Joint Working Group will be formed under the Transportation Sector GCC/Transportation SCC and will be comprised of one member from each modal GCC and SCC or their designate and invited measurement professionals. Under the leadership of TSA’s lead measurement organization, the Group will operationalize measures, establish data sources, data collection and verification procedures, set measurement policy for the TSSP, and approve supporting procedures. This entity may also require standardization of certain measurement practices from data contributors across the sector. The Measurement Joint Working Group will communicate regularly with Transportation Sector GCC/Transportation SCC members to ensure that working group progress and plans are fully transparent and coordinated with the members. In addition, work products of the Measurement Joint Working Group will be submitted, when appropriate, to the overarching Transportation Sector GCC/Transportation SCC for approval.

Measures. The Outcome Monitoring methodology as exemplified in Figure D3-2, Outcome Model, demonstrates working down from the national and multi-modal (sector) goals to determine outcomes and their respective measures.

Figure 3 Outcome Model



The Transportation Sector’s metrics have been segmented into two categories

1. Core:

As discussed in chapter 6 of the TSSP, core NIPP metrics are common across all sectors and focus on measuring risk reduction progress in the sector. These measures are often descriptive statistics (counts)

2. Sector-specific:

- Enhanced Security Measures for Highly Hazardous Materials: There is no statutory mandate to identify high risk hazardous materials or to require enhanced security measures. TSA is taking a risk-based approach to identify high risk substances and working with industry and government stakeholders to develop voluntary measures to reduce the risk.
- Develop risk-based approach to targeting CSRs, and increase from 2 a month the number of CSR conducted

3.6 Transportation Sector Goals and Objectives

Goal 1: Prevent and deter acts of terrorism using or against the U.S. transportation system

1A: Implement flexible, layered, and unpredictable security programs using risk management principles.

Supported by Section 4.1 Program #s – 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 18

1B: Increase vigilance of travelers and transportation workers.

Supported by Section 4.1 Program #s – 1, 2, 3, 4, 5, 6, 7, 8, 12, 14, 16, 17, 18

1C: Enhance information and intelligence sharing among transportation security partners.

Supported by Section 4.1 Program #s - 3

Goal 2: Enhance resiliency of the U.S. transportation system

2A: Manage and reduce the risk associated with key nodes, links and flows within critical transportation systems to improve overall network survivability.

Supported by Section 4.1 Program #s – 1, 2, 3, 11, 12, 13, 16

2B: Ensure the capacity for rapid and flexible response and recovery to all-hazards events.

Supported by Section 4.1 Program #s – 1, 2, 3, 13

2C: Implement risk-based measures to improve the redundancy and robustness of key nodes, links, and flows.

Supported by Section 4.1 Program #s - 1, 2, 3

Goal 3: Improve the cost-effective use of resources for transportation security

3A: Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria.

Supported by Section 4.1 Program #s – 2, 3, 4, 5, 8, 9, 13, 14, 15, 16, 18

3B: Ensure robust sector participation as a partner in the development and implementation of public sector programs for Critical Infrastructure/Key Resource protection.

Supported by Section 4.1 Program #s – 3, 7

3C: Improve coordination and risk-based prioritization of transportation sector security Research, Development, Test and Evaluation efforts.

Supported by Section 4.1 Program #s – 3, 8, 15, 18

3D: Align risk analysis methodologies with Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the National Infrastructure Protection Plan.

Supported by Section 4.1 Program #s – 7

4 Program Management

The Highway GCC, via a GCC subgroup, will facilitate the coordination and periodic update of this modal implementation plan. Subgroup meetings will be held with interested members of the GCC. In addition, the GCC will coordinate review and updates to this plan with the SCC. Once a year, the GCC and SCC will submit revisions for the Highway Infrastructure and Motor Carrier Modal Annex. Every three years, the GCC and SCC will do a complete rewrite of the Annex and will update the Annex as required or necessary.

5 Security Gaps

Security Plans

Security plans throughout the highway stakeholder community are insufficient. There are few voluntary standards or guidance that reduce vulnerabilities and enhance overall security. TSA is drafting Security Action Items (SAI) that are voluntary practices designed to improve security. By developing and distributing these voluntary standards to the highway transportation industry partners, they will be able to mitigate security gaps in the following categories: inadequate plans, policies, and procedures; inadequate training; inadequate access controls; inadequate physical security assets; insufficient security technology and equipment; inadequate communications security; and inadequate information security.

CDL Driver Threat Assessments

Although Security Threat are required for drivers applying for or renewing a Hazardous Materials Endorsement (HME) on their Commercial Drivers License (CDL), CDL holders do not receive a security background check as a part of the licensing process..

Background checks on all CDL holders could reduce the likelihood that a potential security risk would have legal access to trucks and cargo in order to carry-out a terrorist or otherwise harmful act. Large vehicles could be used as vehicle borne improvised explosive devices (VBIED) against critical targets such Oklahoma City and the 1993 attack against the World Trade Center. Additionally, the lack of secure CDL oversight provided to the agricultural industry by the so-called “farm exemption” in motor carrier regulations leaves a gap in HAZMAT and security regulation coverage. Farm vehicles are capable of transporting dangerous chemicals that could be used to make explosives such as ammonium nitrate and other hazardous materials.

HAZMAT Carriers

DOT's HM232 (49 CFR 172.800) requires shippers and carriers of certain highly hazardous materials to develop and implement security plans. However, there are still security gaps that exist in the protection of HAZMAT on the Nation's highways. HAZMAT carrier security gaps include the following: inadequate plans, policies, and procedures; inadequate training; inadequate access controls; inadequate physical security assets; and insufficient security technology and equipment. Research and development projects would assist in closing these gaps by providing enhancements in the protection of facilities, conveyances and critical infrastructure. Implementing technology and security initiatives would also reduce the existing vulnerabilities with regard to the transport of HAZMAT. The Federal Government will continue to review the potential use of technology standards for commercial vehicles carrying high-risk cargoes.

Security Training and Awareness

There is a lack of security-related domain awareness in the areas of the Commercial Driver License (CDL) schools, motorcoach and commercial truck industries, and school bus organizations. Programs to address this gap include Highway Watch, School Bus Watch, School Transportation Security Awareness, Federal Law Enforcement Training Center (FLETC) Roadside Law Enforcement Transportation Security Awareness, and the Hazmat Motor Carrier Security Self-Assessment Training Project. However, such programs do not cover the entire spectrum of highway transportation. More

comprehensive security training and awareness programs would ensure that highway transportation and law enforcement personnel are better prepared to address these gaps.

School Bus Security Training:

There is a lack of sufficient security training for the School Bus industry in the United States. Although there are over 500,000 School Bus employees, there are extremely limited numbers of security training curriculums designed specifically for this critical transportation community. Additional and more comprehensive training is needed to cover this large population. The lack of training and security awareness is a substantial gap that, when addressed, would greatly enhance security for the operators, the passengers, and the public in general. TSA is beginning to address this training gap with support for two programs: the School Transportation Security Awareness program, and the School Bus Watch program (a grant funded program run by the American Trucking Associations). However, increased focus in the areas of security awareness training that would most reduce this gap is prevention and protection training, communication strategies, and response and recovery training.