SECURING THE U.S. TRANSPORTATION INFRASTRUCTURE

BY FRANK GALLOWAY

TranSystems

EXPERIENCE | Transportation

INTRODUCTION

From energy installations that power neighborhoods, to transportation networks that move people around communities and countries, to facilities that provide safe drinking water, Critical Infrastructure and Key Resources (CI/KR) are an important part of daily life. CI/KR is an umbrella term referring to the assets of the United States that are essential to security, public health, safety, economic vitality, and a high standard of living.

Homeland Security Presidential Directive (HSPD) 7 established a policy to identify and prioritize U.S. critical infrastructure and key resources, and to prepare for, protect, or mitigate against a terrorist attack or other hazards against an element of the CI/KR. CI/KR is divided into 18 separate sectors, as diverse as agriculture and food, emergency services, and cyber networks. For each sector, a Sector-Specific Plan (SSP) has been created that details how the National Infrastructure Protection Plan (NIPP) risk management framework can be applied to the risk landscape of each sector.

This paper focuses on initiatives designed to protect the following sectors which TranSystems' clients own or operate: Maritime, Mass Transit / Passenger Rail, Freight Rail, and Highways. The information contained herein derives from the NIPP and the Transportation Systems Sector Specific Plan. [1]

TranSystems, which specializes in transportation consulting and design solutions for these market sectors (among others), also has a line of business directly focused on security. This combination of transportation and security expertise assists our clients in planning and implementing security upgrades – and can help them obtain the federal grant proposals available for financial assistance.

TRANSPORTATION SECURITY ENVIRONMENT

The Transportation Systems Sector comprises all modes of transportation (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline). It is an interdependent networked system that moves millions of passengers and millions of tons of goods. The transportation network is critical to maintaining the high standard of living and economy of the U.S. The transportation network is comprised of approximately 4 million miles of roads and highways, more than 100,000 miles of

[1] *Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan. May, 2007. Accessed February 25, 2010 from http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf*

The strategy focuses onimplementing multiple layers of security to defeat and deter the more plausible and dangerous forms of attack against the transportation network.

rail, 600,000 bridges, more than 300 tunnels and numerous sea ports, 2 million miles of pipeline, 500,000 train stations, and 500 public-use airports.

The sector's security risks are best illustrated by recent attacks using the global transportation network; the September 11, 2001 attacks on the World Trade Center and the Pentagon; the 2005 London bombings, the coordinated attack on four commuter trains in Madrid in 2004, and the foiled 2006 plot in the United Kingdom targeting airlines bound for the U.S. Taken together, the risk from terrorism and other hazards demands a coordinated approach involving all sector stakeholders.

TRANSPORTATION SYSTEM SECTOR SPECIFIC PLAN

Given the reality that terrorists will continue to target the transportation network, the U.S. government implemented a Systems-Based Risk Management (SBRM) strategy that lays out a strategic framework to improve the sector's risk management posture. The strategy focuses on implementing multiple layers of security to defeat and deter the more plausible and dangerous forms of attack against the transportation network.

The National Infrastructure Protection Plan (NIPP), signed in June 2006 as a requirement of Homeland Security Presidential Directive 7 (HSPD-7), obligates each critical infrastructure and key resources (CI/KR) sector to develop a Sector-Specific Plan (SSP) that describes strategies that protect the Nation's CI/KR, outline a coordinated approach to strengthen their security efforts, and determine the appropriate programmatic funding levels. The Transportation System's SSP establishes a strategic approach based on the tenets outlined in the NIPP and the principles of Executive Order 13416, *Strengthening Surface Transportation Security*.

The Transportation Systems SSP describes the security framework that enables stakeholders to make effective and appropriate risk-based security and resource allocation decisions. The strategic plan defines a vision and mission statement, coupled with targeted goals and objectives to which operational and tactical efforts are anchored.

Stakeholders are actively developing methods to improve their operational security and overall resilience. However, since the Transportation Systems Sector is segmented by individual modes, an increased emphasis is needed on a risk-based approach across the entire transportation spectrum. The sector's risk management approach reflects a combined top-down and bottom-up effort.

Figure 1-1 illustrates the dynamic and collaborative risk assessment process and those involved

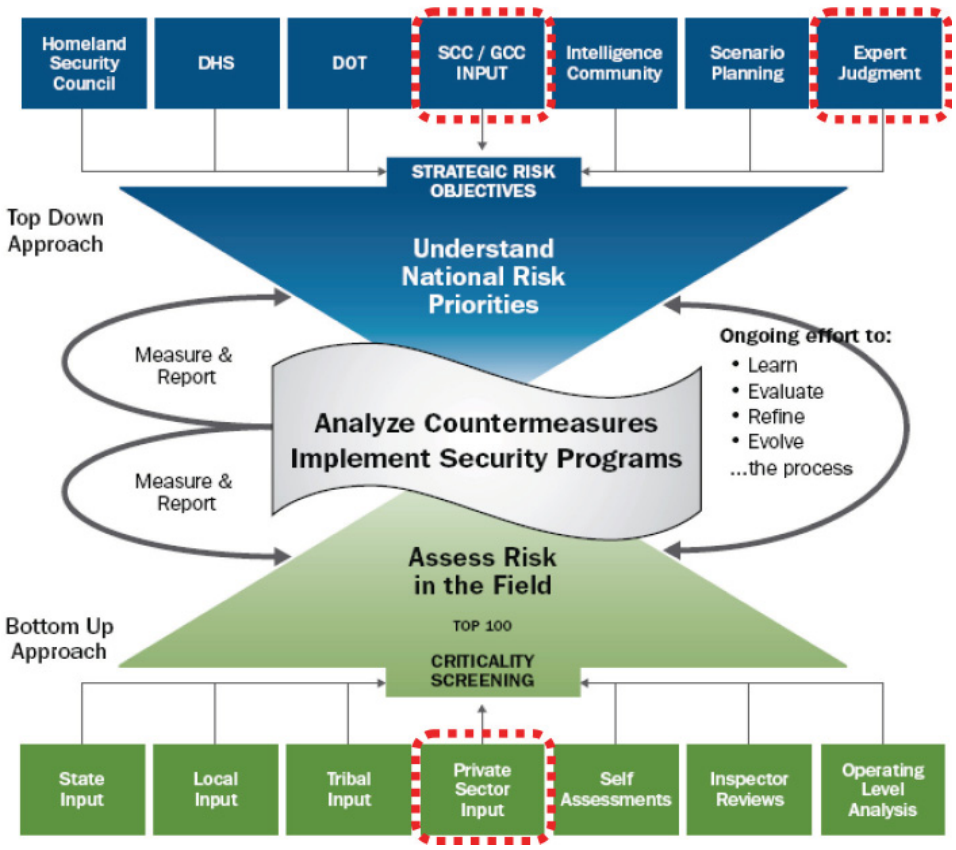


Figure 1-1 Integrated Top-Down, Bottom-up Risk Assessment Cycle; SCC = Sector Coordinating Council; GCC = Government Coordinating Councils

in determining which risks will be identified, analyzed, prioritized, and addressed. The groups outlined in red indicate potential areas where TranSystems can help our client companies influence security in the transportation sector.

SECURITY PARTNERS

The term "security partners" as used in the NIPP includes all levels of government (Federal, State, Territorial, local, and tribal), regional organizations, international partners, and private sector owners and operators. The Transportation Systems Sector partnership model facilitates effective coordination between government and the private sector. Through this partnership, all sector security partners have roles and responsibilities in developing a robust SSP that is representative of their interests. TSA was assigned responsibility as the SSA for the Transportation Systems Sector. The USCG was designated the SSA for the Maritime mode. TSA and USCG have the responsibility to implement HSPD-7 through the NIPP Sector Partnership Model.

SECTOR COORDINATING COUNCILS

Sector Coordinating Councils (SCC) are self-formed councils composed of private sector representatives of infrastructure owners, operators, and related trade associations. Through the transportation SCC framework, private sector participants can provide input to the GCC to help refine and finalize the sector goals, develop the Transportation Systems SSP, and develop mode-specific implementation plans and programs to achieve the sector's goals. Modal SCCs for each transportation mode have been established (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline). TranSystems' can help our clients to protect their assets through participation on an SCC.

OVERVIEW OF THE TRANSPORTATION SYSTEMS SECTOR SBRM METHODOLOGY

Shifting from Assets to SYSTEMS: A systems-based approach examines how assets and systems interact with each other and the negative effects one could have on another if disrupted.

Shifting from Reactive to ADAPTIVE: Flexible security measures and improved information sharing greatly enhance the sector's ability to respond to changing threats.

Shifting from Events to PATTERNS: Although a major consequence is a concern, it is the repetitive occurrence of terrorist attacks worldwide that will show patterns and, in recognizing those patterns, security measures can be identified.

Shifting from Rigid to RESILIENT: "Hardening" is an essential component of protecting critical assets and infrastructure. However, resilience of the transportation system can be improved by increasing its ability to accommodate and absorb unexpected shocks from natural disasters or terrorist attacks without catastrophic failure. Resilience-improving strategies include a wide variety of mitigation activities, including response and recovery activities.

This section of the paper delves into specific transportation sectors, outlining security issues with each, and the focus of national grant programs to address the deficiencies.

The Maritime Sector

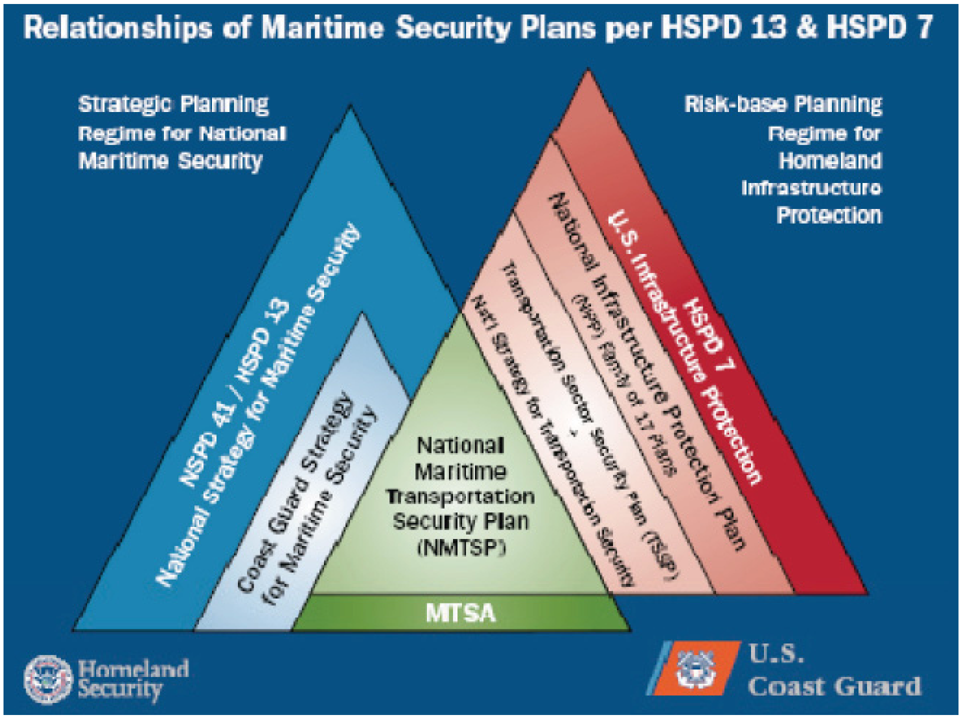
The directives and plans establishing national maritime policy include the following:

- HSPD-7 establishes a national policy for Federal departments and agencies to identify and prioritize U.S. CI/KR and to protect them from terrorist attacks.
- National Security Presidential Directive 41 (NSPD-41)/HSPD-13 is a holistic approach to maritime security missions comprised of the NSMS and eight supporting plans to ensure the safety and economic security of the United States.
- The National Maritime Transportation Security Plan (NMTSP) implements 10 statutory requirements of MTSA and creates a three-tier maritime security planning regime.

MARITIME SECURITY GUIDELINES AND REGULATIONS

Security guidelines are recommended activities, implemented on a voluntary basis, that enhance the security of the MTS.•

- **The Container Security Initiative (CSI):** CSI is a series of bilateral, reciprocal agreements that, among other things, positions CBP personnel at selected foreign ports to pre-screen U.S.-bound containers.
- **The Customs-Trade Partnership Against Terrorism (C-TPAT):** Under CBP's layered, defense-in-depth strategy against terror-ism, C-TPAT is the CBP initiative that partners, on a voluntary basis, with members of the trade community. CBP and willing members of the trade community collaborate to better secure the international supply chain to the United States in support of homeland security. C-TPAT is one of CBP's initiatives that helps the agency achieve its twin goals: security and facilitation of trade moving into the United States.

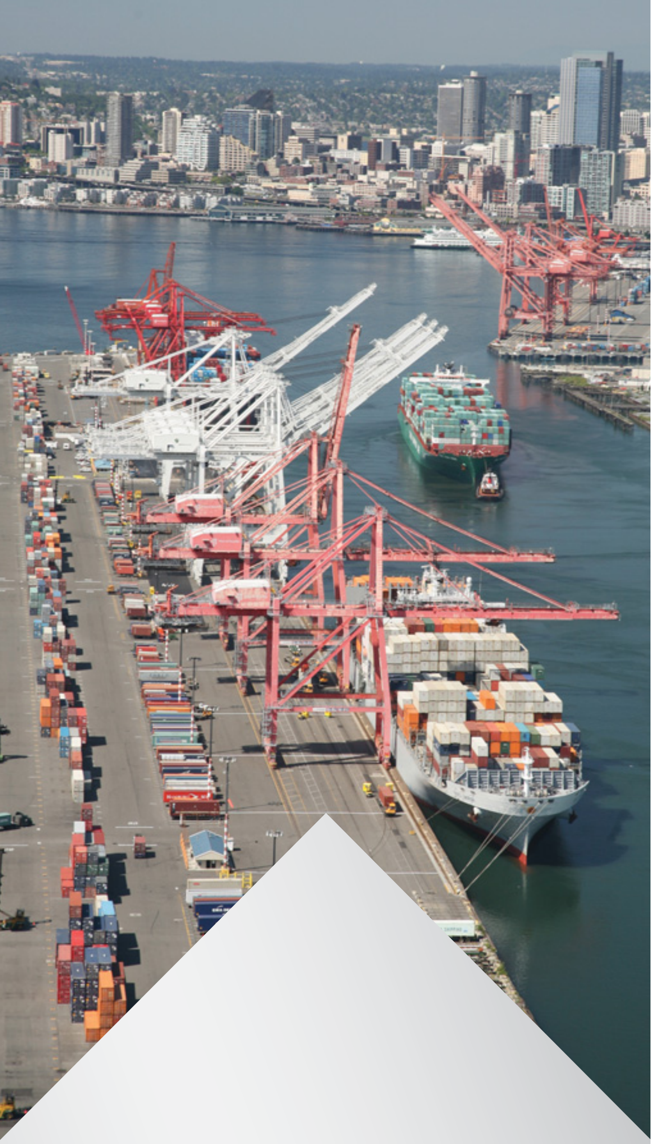

Relationships of Maritime Security Plans per HSPD 13 & HSPD 7
Strategic Planning Regime for National Maritime Security
Risk-base Planning Regime for Homeland Infrastructure Protection
NSPD 41 / HSPD 13
National Strategy for Maritime Security
Coast Guard Strategy for Maritime Security
National Maritime Transportation Security Plan (NMTSP)
MTSA
HSPD 7
U.S. Infrastructure Protection
National Infrastructure Protection Plan
(NIPP) Family of 17 Plans
Transportation Sector Security Plan (TSSP)
+
Nat'l Strategy for Transportation Security
Homeland Security
U.S. Coast Guard

Source: U.S. Coast Guard

- **SafePort Act:** The Security and Accountability For Every Port Act of 2006 (SAFE Port Act) is a comprehensive maritime and cargo security law designed to strengthen port security across the Nation by establishing improved cargo screening standards, providing incentives to importers to enhance security measures, and implementing a framework to ensure the successful resumption of shipping in the event of a terrorist attack, while preserving the flow of commerce. The act establishes interagency operational centers for port security coordination and timetables and procedures for expediting the nationwide launch of the Transportation Worker Identification Credential (TWIC) program. It codifies a number of existing DHS cargo security programs, such as the CSI and C-TPAT programs. The act offers a plan to examine containers entering the United States for radiation and WMDs and provides for improvements in the Automated Targeting System.

Maritime Grant Programs

As a component of the Infrastructure Protection Program (IPP), the Port Security Grants Program (PSGP) seeks to assist the Nation's ports in obtaining the resources and capabilities required to support the National Preparedness Goal and the associated National Priorities. Through its focus on port-wide risk management planning and domain awareness in the port environment, PSGP directly ad-



The Port Security Grants Program (PSGP) seeks to assist the Nation's ports in obtaining the resources and capabilities required to support the National Preparedness Goal and the associated National Priorities.

dresses six of the seven National Priorities:

1. Expanding regional collaboration;
2. Implementing the National Incident Management System (NIMS) and the National Response Plan (NRP);
3. Implementing the NIPP;
4. Strengthening information-sharing and collaboration capabilities;
5. Enhancing interoperable communications capabilities; and
6. Strengthening chemical, biological, radiological, nuclear, or (high-yield) explosive (CBRNE) detection and response capabilities.

In addition, PSGP also supports strengthening emergency operations planning and citizen protection capabilities, and assists in addressing security priorities specific to the port environment. PSGP uses a port-wide risk management program as part of urban area and State efforts. The process is patterned after the risk management framework articulated in the NIPP. Adopting a deliberate risk management planning process enables the FMSC and AMSC to make security enhancement decisions in the context of strategic security goals, supported by clear, measurable objectives. This process allows port area security needs to be integrated into the broader national risk management framework of the NIPP, into the regional planning construct that forms the core of the Urban Area Security Initiative (UASI) program, and into statewide initiatives.

Similar to MTSA, the SAFE Port Act of 2006 requires that each grant be used to supplement and support, in a consistent and coordinated manner, the applicable Area Maritime Transportation Security Plan. Each grant is also coordinated with any applicable State or urban area homeland security plan. The act also states that PSGP must take into account national economic, energy, and strategic defense concerns based on the most current risk assessments available.

Mass Transit Sector

The Transportation Security Administration (TSA) focuses particular attention on six transit security fundamentals that provide the foundation for a successful security program:

1. Protection of high-risk underwater/underground assets and systems;
2. Protection of other high-risk assets that have been identified through system-wide risk assessments;
3. Use of visible, unpredictable deterrence;
4. Targeted counterterrorism training for key frontline staff;
5. Emergency preparedness drills and exercises; and
6. Public awareness and preparedness campaigns.

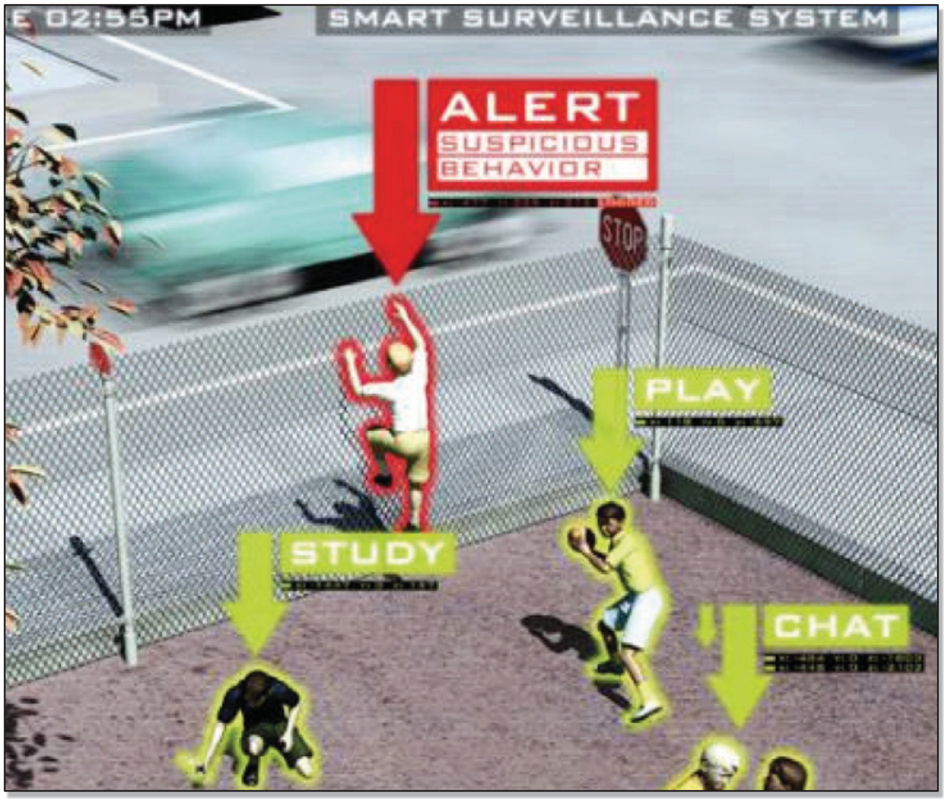
MASS TRANSIT SECURITY GUIDELINES AND STANDARDS

- **Security Action Items:** The 17 Security and Emergency Management Action Items (Security Action Items [SAI]) cover a range of areas, including security program management and accountability, security and emergency response training, drills and exercises, public awareness, protective measures for Homeland Security Advisory System (HSAS) threat levels, physical security, personnel security, and information sharing and security. They are accessible on the FTA and TSA public Web sites and the Public Transit portal of HSIN.
- **Security Standards Development:** The Federal Government is engaging with the APTA Security Standards Policy and Planning Committee to develop security standards.
- **Security Directives:** TSA issued two security directives applicable to mass transit and passenger rail systems in the aftermath of the attacks on commuter trains in Madrid in March 2004. The directives, designated SD RAILPAX-04-01 and SD RAILPAX-04-02, mandate specific measures intended to enhance the security of the Mass Transit and Passenger Rail Mode.

MASS TRANSIT GRANT PROGRAMS

The application of risk-based priorities is institutionalized in regulations governing the Transit Security Grant Program (TSGP), mandated under the SAFETEA-LU rule. The rule emphasizes the enhancement of capabilities in six core transit security fundamentals:

1. **Protection of high-risk underwater / underground assets and systems.** Because of the consequences of IED attacks in an enclosed environment where there may also be large concentrations of riders, protecting riders and the integrity of the transit system against such attacks is essential. Transit agencies should focus countermeasures on programs that can prevent an attack or mitigate the consequences of an incident. Active coordination and regular testing of emergency evacuation plans can also greatly reduce loss of life.
2. **Protection of other high-risk assets that have been identified through system-wide risk assessments.** It is imperative that transit agencies focus countermeasure resources on their highest risk,



highest consequence assets. For example, a system-wide assessment may highlight the need to segregate critical security infrastructure from public access. One solution could be an integrated intrusion detection system, controlling access to these critical facilities or equipment. Transit systems should consider security technologies to help reduce the burden on security manpower. For example, using smart CCTV systems in remote locations can help free up security patrols to focus on more high-risk areas.

3. **Use of visible, unpredictable deterrence.** Visible and unpredictable security patrols have proven to be very successful for instilling confidence and calm in the riding public and, most importantly, in deterring attacks. These kinds of patrols, especially those employing explosives detection canine teams or mobile screening or detection equipment, represent effective means to prevent or deter IED attacks. Security patrols should be properly trained in counterterrorism surveillance techniques. An understanding of terrorist behavior patterns helps security patrols more effectively intervene during terrorist surveillance activities or the actual placing of an IED.

4. **Targeted counterterrorism training for key frontline staff.** Appropriate training enhances detection and prevention capabilities and ensures a rapid, prepared response in the first critical minutes after an attack—steps that can significantly reduce the consequences of the attack. For example, well-trained and well-rehearsed operators can help to ensure that if an under-ground station has suffered a chemical agent attack, trains—and the riding public—are quickly removed from the scene, thus reducing their exposure and risk.

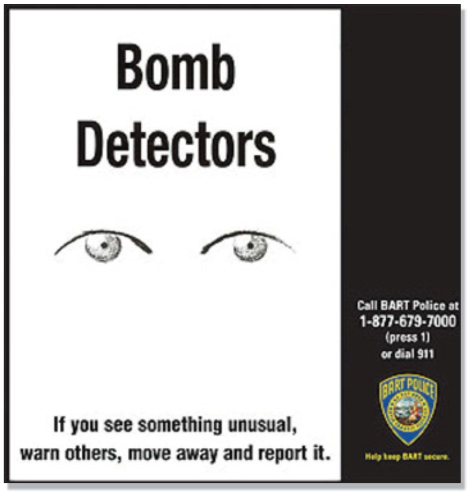
5. **Emergency preparedness drills and exercises.** Experience has taught transit agencies that well-designed and regularly practiced drills and exercises are fundamental for rapid and effective response and recovery. Transit agencies should develop meaningful exercises, including covert testing, that test their response effectiveness and how well they coordinate with first-responders. In addition to large regional drills, transit systems should also conduct regular, transit-focused drills. Drills should test response and recovery to both natural disasters and terrorist attacks.

6. **Public awareness and preparedness campaigns.** Successful security programs in all industries understand the value and power of the public's eyes and ears. Awareness programs should be well-designed and employ innovative ways to engage the riding public to become part of their "transit security system." Advertisement campaigns, using media and celebrity support, have proven to be very successful. Including the riding public in preparedness and evacuation drills has also been shown to be effective in raising public awareness. A transit agency's awareness campaign should also extend to its employees. Appropriate counterterrorism training, coupled with a strong security awareness campaign, will yield significantly heightened security awareness in transit systems.

MASS TRANSIT AND PASSENGER RAIL SECURITY GAPS

The following security gaps are currently addressed in various stages in FTA and TSA programs and processes.

- Information Sharing
- Employee Security Training
- Security Awareness Campaigns
- Research and Development and Technology Deployment
- Mitigation Strategies for Underwater / Underground Tunnels
- Drills and Exercises



HIGHWAY INFRASTRUCTURE AND MOTOR CARRIER

The U.S. Highway Infrastructure and Motor Carrier assets include, but are not limited to, signature bridges, major tunnels, operations and management centers, trucks carrying hazardous materials (HAZMAT), other commercial freight vehicles, motor coaches, school buses, and key intermodal freight transfer facilities. 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.

PRIORITIES AND PROGRAMS

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 Transportation Systems SSP identifies a number of goals and critical voluntary and mandatory programs that incorporate elements to target and assess risk, and secure the Highway Transportation System.

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

- Standardized Risk Assessment and Risk Mitigation Approaches
- Corporate Security Review (CSR) Program
- Security Action Items (SAI)
- FHWA Security Self-Assessment Tool
- Enhance Owner/Operator and Law Enforcement Awareness and Training
- Consolidate Driver Threat Assessments and Credentialing Programs
- Security Plans and Training
- FHWA Security and Emergency Management Professional Capacity Building Program

Goal 2: Enhance the resilience of the transportation system:

- Integrate Security Measures Into the Design of the Nation's Transportation Network
- FHWA-Supported Security R&D Program
- Explore the Use of Existing Grant Programs to Support Critical Highway Infrastructure Security Improvements
- FMCSA Hazardous Materials Safety Permit Program.

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

- Highway Infrastructure and Motor Carrier GCC and SCC
- Trucking Security Program (TSP)
- Infrastructure Protection Program: Intercity Bus Security Grant Program (IBSGP)
- Research the Viable Use of Current and Emerging Security Technologies

SECURITY GAPS

- Security Plans
- Commercial Driver's License (CDL) Driver Security Threat Assessments
- HAZMAT Carrier
- Security Training and Awareness
- School bus Security Training

PROTECTING CRITICAL MOBILITY ASSETS

The principal threat against highway physical assets is explosive attacks on key links such as bridges, interchanges, and tunnels. Nationwide, approximately 450 bridges and 50 tunnels meet relevant criteria as critical assets. While full asset protection is not feasible, reasonable program objectives include the deterrence of terrorist attacks by (1) adding new and clearly visible security features and reducing vulnerabilities, and (2) minimizing the potential for damage in the event of an attack.

Minimize time-on-target for terrorists via installation of real-time intrusion detectionand surveillance systems.

The overall practical objective of the proposed security program is, therefore, not to provide full protection, but to discourage terrorist attack through visible security and reduced vulnerability, as well as to minimize damage in the event of an attack. To protect these assets, the following countermeasures are proposed as retrofits on critical bridge, interchange, and tunnel assets:

- Maximize potential explosives placement standoff distance to key structural members or mechanical systems via various types of barriers.
- Deny access to locations where placement of explosives would affect points of structural integrity and vulnerability for infiltration of mechanical systems through the installation of locks, caging, and various types of fencing.
- Minimize time-on-target for terrorists via installation of real-time intrusion detection and surveillance systems.
- Selectively protect the structural integrity of key members against collapse by strengthening key substructure members and blast shielding.

In addition, these strategies are also assumed to be routinely applied to larger bridges as they undergo their normal reconstruction cycle. TranSystems bridge designers would do well to follow these countermeasures in the planning phase of bridge design.

ENHANCING TRAFFIC MANAGEMENT CAPABILITIES

Many of the nation's larger metropolitan areas are already installing advanced traffic management systems to better manage normal congestion. Expanding deployment of these "intelligent transportation systems" (ITS) is under discussion as a focus of current AASHTO and FHWA (Federal Highway Administration) Reauthorization concepts.

Systematic region-wide deployment of such systems could also substantially enhance the ability of metropolitan roadway systems to support terrorism-related evacuation and emergency response. Seventy-eight metropolitan areas with populations over 550,000 are identified for initial implementation. These 78 metro areas collectively encompass 10,500 miles of freeways and expressways and 16,000 miles of signalized principal arterials. In addition, 1,800 miles of connector routes on the Department of Defense Strategic Highway Network (STRAHNET) are included in this initiative because they link to highway-dependent military installations.

The improved evacuation and emergency access capabilities are achieved by the following program:

- Deployment of ITS technologies on the applicable roadways, including (1) automatic vehicle detection, (2) camera surveillance, and (3) variable message signs – together with

their integration into existing traffic management centers.

- Establishment of nine new regional security guidance centers capable of issuing real-time, event-responsive routing directives during emergencies based on remote imaging, incident tracking, and dynamic routing technologies.

Total costs for this initiative are estimated at $5.6 billion over the six-year period, including $3.7 billion in capital costs and $1.9 billion for O&M.[3]

Freight Rail Sector

The challenge to securing freight rail is protecting against an unpredictable threat environment without slowing down the movement and free flow of commerce. While no specific threat or intelligence points to the freight rail sector, the potential exists for the freight rail system to be manipulated as a target for terrorism or as a delivery system for a weapon of mass effect.

U.S. freight railroads move more freight than any other rail system in the world. U.S. railroads operate more than 140,000 miles of track and earn $42 billion in annual revenues. Forty percent of intercity freight travels by rail, including 64 percent of the coal bound for the nation's electric utilities.

GOALS, OBJECTIVES, AND PROGRAMS / PROCESSES

DHS has outlined three goals for the transportation sector. Each goal is supported by objectives that assist in focusing the mode's programs and initiatives to meet that specific goal.

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

- Implement flexible, layered, and effective security programs using risk management principles.
  - High Threat Urban Area (HTUA) Rail Corridor Assessments
  - Comprehensive Reviews
  - Corporate Security Reviews
- Increase the vigilance of freight rail workers
- Enhance information and intelligence sharing among freight rail security partners

[3] *Ham, D. & Lockwood, S. (2002). National Needs Assessment for Ensuring Transportation Infrastructure Security. NCHRP Project 20-59, Task 5, National Cooperative Highway Research Program, Transportation Research Board.*

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

- Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability
- Enhance the capacity for rapid and flexible response and recovery to all-hazards events

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

- Align sector resources with the highest priority security risks using both risk and economic analyses as decision criteria
- Ensure robust sector participation in the development and implementation of public sector programs for freight rail protection
- Ensure coordination and enhanced risk-base prioritization of research, development, testing, and evaluation efforts

PRIVATE SECTOR PROGRAMS AND PROCESSES

- AAR Terrorism Risk Analysis and Security Management Plan
- The Emergency Response Training Center at the Transportation Technology Center, Inc. (TTCI)
- TIH Shipping Industry Partners
- Transportation Community Awareness and Emergency Response (TRANSCAER)
- Railway Alert Network (RAN)
- AAR Operations Center

SECURITY GAPS

- The presence of standing, unattended, loaded TIH cars in HTUAs
- The lack of robust standardized security planning at the corporate and facility levels for all railroad operations.
- A gap in worker security awareness training

SECURITY GUIDELINES AND SECURITY STANDARDS

DOT Security Plan Regulation:	49 CFR 172.800
Department/Agency:	PHMSA and FRA
Goal: Prevent and deter acts of terrorism using or against the transportation system	
DOT requires shippers and carriers of HAZMAT that presents a transportation security risk to develop and implement a security plan. The security plan must be based on an assessment of possible transportation security risks.	

48-Hour Rule:	49 CFR 174.14
Department/Agency:	PHMSA and FRA
Goal: Prevent and deter acts of terrorism using or against the transportation system	
DOT requires that each shipment of HAZMAT be forwarded "promptly and within 48 hours (Saturdays, Sundays, and holidays excluded)" after acceptance of the shipment by the railroad carrier.	

Hazardous Materials:	Enhancing Rail Transportation Safety and Security for Hazardous Materials Shipments Notice of Proposed Rulemaking (NPRM), published on December 21, 2006, 49 FR 76834
Department/Agency:	PHMSA and FRA
Goal: Prevent and deter acts of terrorism using or against the transportation system.	
DOT and the TSA revised the requirements in the Hazardous Materials Regulations that are applicable to the safe and secure transportation of specified HAZMAT transported in commerce by rail. Specifically, the regulations require that rail carriers compile annual data on specified shipments of HAZMAT. PHMSA proposed that data will be used to analyze safety and security risks along rail transportation routes where specified materials are transported, assess alternative routing options, and make routing decisions based on those assessments.	

Rail Security:	NPRM, published on December 21, 2006, 49 FR 76852
Department/Agency:	TSA
Goal: Prevent and deter acts of terrorism using or against the transportation system	
TSA proposed requiring freight railroad carriers and fixed-site rail HAZMAT facilities that ship or receive in an HTUA specified categories and quantities of HAZMAT to appoint a security coordinator and report suspicious incidents. TSA proposed that freight railroad carriers and the affected rail HAZMAT facilities report to TSA, upon request, the location and shipping information of certain rail cars containing specified categories and quantities of HAZMAT. TSA proposed measures that would ensure a positive and secure exchange of custody and control of rail cars carrying specified categories and quantities of HAZMAT.	

CONCLUSION

Today, years later, the images of the World Trade Center attack linger. We vow, "never again." By taking advantage of the groundwork laid by Federal security planning and incentives, TranSystems' clients can make their assets more secure and the public safer from assaults on our transportation infrastructure.

TranSystems

EXPERIENCE | Transportation

For more information about our services, please contact:
1.800.505.9221 • Reference: MS-80