Transportation Infrastructure Protection and Emergency Management

State DOT Workshop Results—Good Practices and Key Concerns

AASHTO
The Voice of Transportation

Transportation Security Administration

U.S. Department of Transportation
Federal Highway Administration

CONTENTS

Text by Karen Haas
Design by Jane Perini
Manifest Inc., Rockville, MD

INTRODUCTION

This document, published by the American Association of State Highway and Transportation Officials (AASHTO), summarizes the results of a series of five State Department of Transportation (State DOT) workshops jointly sponsored by the Federal Highway Administration (FHWA) and the Transportation Security Administration (TSA), in cooperation with AASHTO. Workshop locations and dates were:

- Springfield, IL, October 2006
- Iselin, NJ, December 2006
- San Francisco, CA, June 2007
- Tampa FL, July 2008
- Kansas City, MO, March 2009

The workshops were structured to gather input from the States about their key concerns related to Infrastructure Protection and Emergency Management; to share Good Practices; and to disseminate information to the States, including key findings from TSA Corporate Security Reviews of State DOTs, as well as information about resources available from FHWA, TSA, and the National Cooperative Highway Research Program (NCHRP). The first four workshops brought together colleagues from State DOTs in the immediate multi-State region surrounding the host State. The fifth and final workshop, in Kansas City, was a regional workshop as well, but participants from around the country also were invited to attend, in order to permit discussion of issues from a national perspective.

To facilitate open and frank discussion, workshop participants were told that their comments about sensitive concerns would not be published. In order to honor this commitment to the confidentiality of the discussions, States and participants are not identified in the discussion of Key State Concerns (pages 5-7). On the other hand, in order to facilitate peer exchange, States are identified in the discussion of Good Practices (pages 8-13).

The Resources section of this document (pages 14-16) provides further information about Infrastructure Protection and Emergency Management resources available to States from Federal agencies and other sources.

CROSS-CUTTING ANALYSIS

The workshop results present five snapshots of the State-of-Practice for Infrastructure Protection and Emergency Management, taken over a two-and-a-half year period. Stitching the snapshots together reveals some general "big picture" realities.

Infrastructure Protection—State of Practice

Infrastructure Protection practice varies broadly across the country, as do State DOT perspectives on Infrastructure Protection needs. In States with densely populated major metropolitan regions, or high-risk infrastructure, transportation Infrastructure Protection issues are a major concern to the DOT staff assigned to security issues. While DOT staff may be concerned that the DOT leadership and other State decisionmakers do not consider transportation Infrastructure Protection a priority, staff addresses infrastructure protection risk assessment and mitigation planning functions with increasing sophistication. Implementation of countermeasures is being addressed to the degree that resources and countermeasures are available.

In States that are predominantly rural with few known infrastructure risks, Infrastructure Protection is generally not a priority, especially in comparison with other needs for scarce resources. This tendency is exacerbated by policies that direct Infrastructure Protection funding to high risk areas, which essentially ensures that the more rural and remote States have especially scarce resources for Infrastructure Protection activities. As a result, DOT personnel in predominantly rural States generally are not well versed in risk assessment, planning, or countermeasure implementation. Instead, the emphasis is on All-Hazard Response Preparedness. This participant from a rural State voiced a typical viewpoint:

> "Funding for security is scarce, so the emphasis at our DOT is on taking care of fundamental needs. We are making sure each of our District Offices has an Emergency Operations Center (EOC), and can run the District from their District Office. We maintain back-up power resources, and keep emergency contact lists updated. We also work to stay current with fluid emergency processes at other agencies."

State DOT Role in Emergency Incident Response is Evolving

DOT personnel are becoming more comfortable and proactive in their roles as incident response partners. In the initial workshops, some participants were uncertain of their roles in emergency response. They weren't sure how to approach outreach to partners. In the more recent workshops, participants exhibited increasing assertiveness, including willingness to invite themselves to meetings in order to raise awareness among other responders about why working with the State DOT is important. As a result of increasing comfort with their role in emergency incident response, State DOTs are developing better relationships with other response agencies. There also seems to be a trend toward more cross-state, multi-region meetings. Most participants felt that there is a need to create an operational

culture within DOTs that supports those involved in the transportation aspects of incident response as first responders who are part of a multidisciplinary incident management team, and need to be available 24/7. Some State laws (for example, Arizona, Oregon, and Idaho) recognize DOT personnel as emergency responders, but most do not. The definition of "first responder" used for U.S. Department of Homeland Security (DHS) grants and funding does not include transportation.

Although State DOTs, for the most part, participate in the exercise planning process and the development of emergency plans, there is a need for continual reinforcement of the State DOT role in emergency response and recovery, and recognition of State DOT capabilities and limitations. For example, some States expressed concern that the DOT is not trained and equipped to operate in Chemical, Biological, Radiological, Nuclear (CBRN) environments, but that the DOT might nevertheless be called upon to do so in an emergency.

Partnership Challenges Remain

While progress is being made, many State DOTs still experience challenges in developing good working relationships with incident response partner agencies at the State and local levels. Relationships with law enforcement vary widely. In some States, the DOT and State Patrol work very closely together, while in other States, there is an arms-length relationship. Co-location of law enforcement and transportation personnel in Traffic Management Centers (TMCs) and EOCs seems to foster better working relationships.

To help promote better relationships with State law enforcement agencies and state emergency management agencies, AASHTO's Special Committee on Transportation Security and Emergency Management (SCOTSEM) has been reconstituted to allow three participants from each State. The goal is for each State to have a representative from the DOT; the State law enforcement agency; and State emergency management agency.

A few State DOTs are very proactive in reaching out to local fire, EMS, and law enforcement agencies, with good results, although this requires continual effort due to the large number of local agencies and frequent personnel turnover.

NIMS Training Was a Worthwhile Investment

Initial National Incident Management System (NIMS) training requirements were a challenge for State DOTs, but workshop participants felt that the training investment paid off by increasing awareness of incident response issues and roles.

Multiple Planning Requirements are Challenging

Many State DOTs are struggling to meet requirements for a multitude of planning requirements, including Emergency Support Function (ESF) 1 in the National Response Plan; transportation agency continuity of operations and support for Pandemic and Avian Flu outbreaks; and evacuation planning. In many cases, the individual(s) within the State DOT who is responsible for the transportation agency's input to these plans also has operational responsibility for both routine operations and emergency response.

Need for Regional-Level Planning is Increasingly Recognized

There is a growing recognition of the importance of regional-level planning for Infrastructure Protection and Emergency Management, in order to ensure the safety and security of multiple jurisdictions that share major transportation corridors.

Need to Foster State DOT Access to Security Information in Some States

There seems to be a need to foster information-sharing relationships between State DOTs and the intelligence/law enforcement community in some States where the DOTs complain that they have no access to security information. In other States, the DOTs routinely receive information and work closely with fusion centers, the TSA, law enforcement, and others to analyze information and make decisions about risk mitigation.

Similarly, the process for distributing transportation security information from the Federal to State levels remains an issue. Distribution of various unclassified but marked information from Washington to the State level seems to have improved. But once the information arrives in the State, it seems that in most cases DOTs are not in the loop for information that might be oriented to the highway or transportation system. Most of the confusion seems to stem from the variety of information disclaimers and classifications. A better balance needs to be achieved between the need to protect information and the ability to disseminate it to those who need to be informed.

Some State DOTs expressed initial concern that they were not allowed access to the National Critical Infrastructure List to determine whether any of their assets were on the list. Through workshops, exercises, and other training, most State DOTs are now realizing the need to identify iinfrastructure that is critical to the economy of the State, and the well being of its population, without regard to a national list.

Funding and Resource Challenges

Although FHWA Federal-aid funding can be used to support security and emergency management activities, planners do not have a good understanding of this, and State DOTs often are not willing to use highway funding for security projects or enhancements.

Although the U.S. DHS and TSA have personnel located at State capitals (DHS Protective Security Advisors or PSAs) and at major airports(DHS Federal Security Directors or FSDs), these individuals generally tend to work with State DHS or Office of Emergency Management (OEM) offices and personnel. There is a need to train the PSAs and FSDs about how to develop ongoing working relationships with State DOT agencies and personnel. The training should be tailored to each State.

KEY STATE CONCERNS

Across the country, workshop participants voiced some common concerns. These included:

- Funding and Resources
- Access to Security Information
- Need for Infrastructure Protection Guidance
- Cyberseccurity
- Partnership Challenges
- Emergency Communications and Coordination Challenges
- Planning Challeges

Funding and Resources

Funding and Resources for Infrastructure Protection: Workshop participants from States where Infrastructure Protection risks are considered a major priority expressed strong concern regarding the lack of resources for security, and the fact that security programs are not a priority at most State DOTs. They said it is becoming increasingly difficult to secure decisionmaker support for security programs, as memory of September 11th recedes, States experience continuous turnover in political decisionmakers and senior DOT staff, and budget pressures increase.

Within the State DOTs, personnel assigned to security issues say they lack resources both for security planning, and for countermeasure implementation. This comment is typical:

> "The problem is, there is so much to do every day. Emergency managers have time to plan. But many of our security positions have developed from the operational side. The operational side is very jammed. I hear this lot: 'I don't have time today to worry about Al Qaeda—I have four lanes jammed on the Interstate.' "

At the State, regional, and local levels, funding for security must compete with issues of more direct daily concern to voters. Participants noted that the most convincing tactic for increasing security funding may be to seek resources for security within an All-Hazards Preparedness model.

Funding and Resources for 24/7 Operations: Participants said an operational culture needs to be created within State DOTs to recognize and support the emergency responder role of DOT employees who are involved in incident response. As members of a multidisciplinary incident response teams, DOT responders and their equipment and resources need to be available 24/7.[1] Participants suggested that AASHTO provide talking points and/or marketing materials to help communicate the importance of security and emergency management to policymakers.

Funding and Resources for Evacuation Planning: Some States have had difficulty obtaining funding for evacuation planning. The funding situation is complicated by formulas that limit the proportion of funds that can be retained by the State, versus passed through to local government. Limits on spending of planning funds for State DOT personnel also can be problematic. Some participants called for a dedicated Federal funding stream to assist DOTs in evacuation planning.

Funding Guidance: A few States have been very successful in securing funding from Federal and State sources to support their Infrastructure Protection and Emergency Management programs. Most States, however, are still struggling with this issue. Participants said they need guidance on how to secure funding from available sources.

Pre-event hazard mitigation funding is an area where there is considerable confusion, and more guidance is needed.

Guidance on permissible use of Federal-Aid Highway Program funds also is needed. For example, Federal-Aid funds may be used for evacuation planning, and for purchasing resources needed to control highway access for contraflow operations.

Guidance on how to cost-share projects with emergency response partners also is needed. For example, one State DOT that successfully shared costs with a city police department for a TMC dispatch program was not able to cost-share security enhancements on highways,

---

[1] "Traffic Incident Management responders and resources should be available 24/7" is Strategy #12 of the *National Unified Goal for Traffic Incident Management*. For more information, see http://timcoalition.org/?siteid=41

because co-mingling of law enforcement and transportation funds proved too challenging. It was difficult to create a clean split between enforcement and traffic management in order to justify use of Federal-aid funds, and issues regarding maintenance of the system and data ownership also were problematic.

State DOT Access To Security Information

Some States Lack Access to Security Information: Some State DOTs voiced concerns about lack of access to security information, which leaves them unable to assess threat levels to their system at any given time. Intelligence information tends to become absorbed into secret classifications. Information that could be useful to State DOTs is rated "Not For Distribution," for no apparent reason.

The greatest challenge in information-sharing is with the law enforcement community. In many States, the law enforcement community does not share intelligence and information, and State DOTs are not included in regional information-sharing networks.

Several State DOTs reported that their State Office of Homeland Security does not forward available security information to the State DOT.

Although the TSA has facilitated security clearances for a selected number of State DOT personnel, even when State DOT personnel have secret clearances, those who have the secret information are not able to share it with DOT decisionmakers to convince the decisionmakers of the importance of security.

Some States Do Receive Security Information: On the other hand, some State DOTs do receive security information routinely, from their fusion centers, TSA, State Highway Patrol, the FBI, and other sources. In some States, the fusion center routinely reports intelligence information to the State DOT, and it is up to the State DOT officials to analyze the significance of the information. Some State DOTs work closely with law enforcement and with DHS PSAs in making decisions regarding security.

Procedures for Reporting Transportation System Threats: Procedures for reporting information about transportation information threats is a related concern expressed by some workshop participants. Some State DOTs routinely provide information to their fusion centers. Others try to push information, but find it is not wanted. Several State DOTs reported confusion about who was eligible to report threats through the former Highway Watch® program (TMCs, DOT dispatchers, or DOT drivers). In fact, anyone can report through the new First Observer Program. Call Center personnel will provide feedback to the caller within 72 hours. The 24/7 First Observer Call Center number is 1-888-217-5902.

Need for Infrastructure Protection Guidance

As noted in the Cross-Cutting Analysis (page 2), State DOT's vary widely in their approach to Infrastructure Protection. States that include high-risk infrastructure, and/or densely populated metropolitan regions, are the most vocal in requesting additional guidance as they grapple with issues related to risk assessment, countermeasure identification and implementation, and response planning. Some of the many issues related to this topic include:

- Security Investment Prioritization
- Risk Assessment Methodology
- Security Design Guidance
- Facilities and Equipment Security

Security Investment Prioritization: State DOTs would like more guidance on how to prioritize security investments. Confusion abounds regarding whether to base countermeasure investments on threat levels, risk levels, or resource lev-

els. Some representative concerns voiced by workshop participants:

- We participate in our State's Critical Infrastructure Protection Committee and have completed reviews of transportation infrastructure. We are challenged in ranking the relative criticality of diverse infrastructure and facilities— for example, a border crossing between two countries, or a chemical plant. The issue of governance complicates security planning. Many bridges and tunnels operate under a variety of ownerships and authorities.
- The regional domestic security task forces have instructed the DOT not to take action on to protect their infrastructure from security threats until they get a critical threat. The DOT developed their internal list of critical assets, but DOT personnel did not know whether any of the facilities they are responsible for are on the State or Federal critical infrastructure list.[2] With money as tight as it is, State DOTs are not going to invest a lot in infrastructure protection unless there is a credible threat.

Risk Assessment Methodology: State DOTs use many different methods for assessing the vulnerability of their transportation infrastructure. Some participants suggested that a more uniform approach is needed, in order to make more rational decisions from a national perspective regarding resource allocation. TSA is currently developing guidance regarding baseline mitigation measures to reduce infrastructure risk.

Security Design Guidance: Some States requested guidance regarding design standards for security features. The American Planning Association's (APA's) *Draft Policy Guide on Security* encourages planners to balance security and personal freedom that enhances quality of life.

Facilities and Equipment Security: Security of State DOT vehicles, maintenance equipment, and maintenance stations is a concern, and State practices vary widely. State practices have been documented by TSA in the Corporate Security Reviews (CSRs) conducted by TSA at State DOTs over the past several years.

Cybersecurity is a Growing Concern

Cybersecurity is a growing concern for DOTs. The two major issues are redundancy, and penetration testing (testing against hackers).

In general, there needs to be a balance between operational user requirements and the importance of ensuring overall security and continuity of the IT system. Creating this balance requires frequent user interface with IT personnel to establish user requirements.

The physical security of Information Technology (IT) facilities also is a concern. Many computer rooms are protected by water sprinklers, which would destroy the computer equipment if deployed. Others have no fire protection in the room. It is also common to find computer facilities that are secured by door locks, but vulnerable to easy entry through moveable ceiling panels. TSA has established a Cybersecurity Working Group.

Partnership Challenges

While States vary widely in their partnership practices, some common partnership challenges currently facing State DOTs include:

- Building Partnerships with the Private Sector
- Building Partnerships with Local First Responders
- Working with State Emergency Management and State Law Enforcement

Emergency Communication and Coordination Challenges

The Post-Katrina era has brought overall progress in emergency communication and coordination, but challenges remain. Among them are;

- Emergency Communication and Coordination Between State DOTs
- Communication Between the State DOT and Its Employees During Emergencies
- Communication and Coordination Between State DOT and Other State and Local Emergency Response Agencies

CBRN Guidance is Needed

DOTs are very challenged by issues related to working in, and responding to chemical, biological, radiological and nuclear (CBRN) events. Guidance is needed.

[2] The Federal list of critical transportation infrastructure is classified. The National Infrastructure Protection Plan calls on DOTs to prevent incidents, mitigate them, and restore infrastructure as soon as possible when incidents occur. Because of the difficulties of assessing threats to surface transportation, the trend has been toward consequences-based and/or capabilities-based planning instead of threat-based planning.

GOOD PRACTICES

Security Assessments

- **Texas DOT (TxDOT)** had all of its districts identify critical infrastructure, prioritize the top 10, and analyze the cost-effectiveness of security enhancements. As a result, TxDOT is well positioned to implement security measures promptly if funding becomes available.
- New Jersey's Governor mandated that private-sector transportation authorities conduct site-specific security assessments of critical facilities, and develop a mitigation plan and a site-specific emergency operations plan. The State Attorney General enforced the order. **New Jersey DOT (NJDOT)** identified the facilities that the State considered critical, and NJDOT personnel had the authority to evaluate the vulnerability assessment. The private sector was very cooperative and seemed to appreciation the State's proactive policy.
- **Oregon DOT (ODOT)** identified vulnerable transportation infrastructure using the AASHTO guide. ODOT formed a committee that included the DHS security advisor for Oregon, and through the committee was able to obtain FBI threat assessment data. With assistance from an FHWA expert team, Oregon was able to develop an intruder protection program and obtain DHS funding to implement it.

Facilities Hardening

- Several years ago **Illinois DOT (IDOT)** had a consultant develop risk assessments of all IDOT facilities, and develop a risk mitigation plan. In implementing the plan, bridges have been a major focus in the last several years—they have added lighting, cameras and fences.
- **California DOT (Caltrans)** works with the California Highway Patrol (CHP) to provide trained security patrols for iconic bridge structures. Plans are accessible through regional centers, but disclosure statements must be signed by those who receive the plans. Caltrans was planning to develop a response plan for terrorist-vulnerable bridges, similar to the plan they already have in place regarding procedures for closure of bridges in the event of seismic damage.
- **Ohio DOT (ODOT)** has improved the physical security of

all of its facilities by installing fences, implementing security cards and other measures. All the infrastructure security measures have been paid for with homeland security funds.

- **NJDOT's** bridge design manual was been updated to include protocols for designing security into bridges. NJDOT also developed written protocols for bridge security inspections.
- The **New Jersey State Department of Homeland Security** conducts on-site security audits of private sector transportation facilities. The State worked with private sector transportation partners to develop industry best management practices, which they have distributed to 13 private sector transportation authorities.
- **Colorado DOT (CDOT)** worked closely with tunnel authorities on awareness. For some major structures, they installed setbacks (a "safe zone").

Personnel Security

Some States require background checks for employees and consultants that may include criminal background checks and checks against the terrorist watch list. Some States require contractors to hire security personnel.

Security Training

- **New Jersey** developed security awareness training for every transportation subsector.
- **Minnesota DOT (MnDOT)** requires all employees to attend a four-hour security awareness class.
- **Virginia DOT (VDOT)** has a separate budget for security. They use it for security training as well as for facilities hardening.

Funding

- **New Jersey** is using health funding to convert a rail car into a hospital that could sustain life support for first responders going into a hot zone.
- In **Minnesota,** transportation receives a large share of the State's 20 percent share of Federal Emergency Management Agency (FEMA) Urban Area Security Initiative (UASI) funds. The DOT is represented in the committee that determines how the State's UASI funds will be allocated.
- **New Jersey** State officials worked closely with counties to persuade them to spend local UASI and Highway Safety Improvement Program (HSIP) funds on critical infrastructure protection instead of buying new equipment. One county gave the State money to install surveillance cameras on a State highway. The State uses its 20 percent share for regional initiatives that span all the counties.
- The **Idaho Transportation Department (ITD)** successfully promoted security, safety, and emergency management as part of an overall focus on the improved operational efficiency of the transportation system.

Partnership Building

While it still seems to be more the exception than the rule, a few State DOTs are partnering successfully with private transportation sector organizations to share security and other information.

- In **New Jersey**, the transportation security sector leadership meets at the State level every six months. Every quarter public and private subsector stakeholders meet to share information about intelligence and threats; funding opportunities; and other topics.
- **New Jersey** partnered with CSX rail. They have a tracking system that shows the status of the rail system, including every rail line, and all hazmat material.
- **Tennessee DOT (TDOT)** has also partnered successfully with CSX, as well as Federal Express . During the evacuation from Hur-

ricane Katrina, CSX and Canadian National railroads provided TDOT with reliable information on arrival of evacuees.

- The **Iowa DOT** places high priority on private sector partnerships and participates actively in the Iowa Business Partnership for National Security. Most of Iowa's key transportation resources and critical assets are owned by the private sector. The Iowa DOT wants to share information with the private sector and is exploring techniques for scrubbing data to protect sensitive information while enabling sharing of other important data.

- **Wisconsin DOT (WisDOT)** was considering creating a position for a private sector liaison who would channel information to businesses during emergencies, and solicit emergency resources from the private sector when needed. WisDOT conducted an exercise on pandemic preparedness with the private sector in downtown Milwaukee.

- A few States are actively reaching out to partners in local response agencies, which is especially challenging because there are hundreds of local agencies in each State, with considerable turnover.

- The **Idaho Transportation Department (IDT)** has been successful in cooperating with the fire service in rural areas to develop a fire response plan for remote areas that were formally without fire coverage. These plans establish a fire response to vehicle fires on the Interstate and on State roads.

- **Florida DOT (FDOT)** district personnel are partnering with local law enforcement to fight hate crimes and gang violence. FDOT District 2 field personnel are educated so that they can recognize the meaning of graffiti, both for their own protection—so they can realize when they may be in gang territory—and so they can notify law enforcement prior to removal of the graffiti. Personnel are asked to e-mail a digital photo of any graffiti containing the criminal or extremist symbols, along with information regarding the exact location of the graffiti, to an FDOT liaison, who contacts the county Sheriff's office and files a vandalism complaint. In some counties, a gang detection unit may investigate; other cases may be forwarded to the regional domestic security task force, which forwards to the relevant gang detective unit. There have been incidents where the FDOT report resulted in arrest of gang members. FDOT policy is to remove the graffiti as soon as possible after the report is filed. FDOT personnel were at first hesitant to e-mail the pictures because they were fearful of repercussions for sending crude content on DOT computers. A memo from the executive level reassuring personnel that they would not be fired for reporting graffiti resolved that issue.

- **Missouri DOT (MoDOT)** places priority on relationship-building. MoDOT participates in all National Guard exercises, and in area meetings with emergency coordinators, and also strives to build relationships with local communities.

- **Ohio DOT (ODOT)** works closely with law enforcement and fire agencies, and participates in the multidisciplinary Ohio Quick Clear incident management program. They take an All Hazards approach to incident management and emphasize the safety benefits of quick clearance.

- Several States are working to develop closer bonds to neighboring State DOTs. For example, **WisDOT** has reached out to border States to develop common strategies on the borders, which enables them to leverage existing resources. The South Wisconsin Consortium grew to include Chicago, and multi-State consortia and public/private consortia were under consideration.

Training and Exercises

- **Iowa DOT** regularly holds many types of trainings and exercises. They adapted an Executive Decision Matrix from the National Capital Region that maps out the key information needed within the first 45 minutes of an event, and they exercise a portion of the Executive Decision Matrix with their decisionmakers during each exercise.

- **MnDOT** developed functional exercises with live play, focusing on Statewide objectives as well as objectives developed by each district. They brought in the National Guard, State Patrol, Coast Guard, and others for 30-hour exercises, which was a major resource commitment. The exercises went beyond the tabletop experience to simulate real experiences (such as the death of an employee, or bridges taken out) and the participants had to go out and respond to the incidents. Employee feedback was very positive. One comment said it was the "most valuable training in 33 years of service."

- **Illinois DOT (IDOT)** conducts annual exercises to train personnel how to implement the evacuation plan, the earthquake plan, and other emergency operations plans. The plans are adjusted based on the results of the exercises.

- **Ohio DOT (ODOT)** is emphasizing use of the Incident Command System (ICS) and Unified Command (UC) to help transportation agencies do a better job of managing on-scene operations cooperatively with the response agencies at the scene. ICS training for field transportation personnel is the key to enabling them to be effective in interfacing at the scene.

Coordination

- **Missouri** consolidated Emergency Management and Homeland Security. Both functions involve the same people in most cases, at the State and county level.

- **Minnesota** has a combined Office of Homeland Security and Emergency Management.

- Michigan has a State Homeland Protection Board. **Michigan DOT (MDOT)** successfully advocated a separate Statewide goal for transportation (instead of folding transportation under infrastructure). A stand-alone goal enables transportation to report to the Board separately. Working through the Board provides MDOT with a good communications link to other State agencies on security-related issues.

- The **Kentucky Transportation Cabinet** (Kentucky's transportation agency) reorganized so that the highway safety functions were brought together into one department with two major divisions. One deals with safety and security; the other with traffic safety education.

Communications

- The 12 **Ohio DOT (ODOT)** districts all have emergency operations centers and they all communicate on a common radio frequency, with the State EOC backing up the priory ODOT radio communications system. Transportation has daily communications with the State intelligence group through a secure, password-protected voice communications system.

- **Ohio** is focusing on improving communications by increasing redundancy, and developing better interfaces with Voice-Over Internet Protocol (VoIP), and blackberries. They have established emergency management groups through their computer e-mail system.

- Communications is a top prior-

ity for **Kansas DOT (KDOT)** because KDOT provides communications for the State Highway Patrol. They have a mobile communications unit that can tie in 10 different radio channels to provide interoperable voice communications. KDOT also has 60 handheld communications units that they can distribute to responders. KDOT personnel have Government Emergency Telecommunications Service (GETS) cards that provide priority access to telecommunications lines when the lines are jammed during an emergency.

- **Colorado** has a Statewide radio system that links the Colorado State Patrol, CDOT, 2,300 local jurisdictions and first responder agencies. The Denver metro area is on a different system but there is a gateway patch to that system. DHS grants helped fund the system.

- **New Mexico's** State radio system is provided by the State General Services Department, and links all the State agencies. Each agency has a dedicated frequency, but there also are shared frequencies. An interoperability initiative is under way to link the State system with local responders. For data, the State is still trying to build out the infrastructure on a closed secure system. Information exchange is through secure access encrypted on the Internet.

- **Idaho's** State communications center provides radio frequency and communications resources to link various agencies Statewide (through patches). It also provides dispatch for HAZMAT, homeland security officers, internal DOT dispatch, medevac helicopter dispatch and flight control, and dispatch of emergency medical services (EMS) for half the State. Idaho also has a State panel working on broadband spectrum availability (700 Mhz), but more money is needed in order to make broadband available to public agencies.

- **Arizona DOT (ADOT)** has public safety radios in certain vehicles to help with on-scene coordination. Interoperable communications vans are stationed throughout the State—these vans are able to patch together the different radio systems from various responder agencies. The governor has established interoperability as a strategic initiative, and ADOT is a participant in the Statewide commission on interoperability. The Arizona Interagency Radio System (AIRS) is a Statewide 800 Mhz system that enables all State agencies to communicate with one another. ADOT currently is rebanding its radios to be able to access the Statewide system and other frequencies.

- **Nevada DOT (NDOT)** joined consortia that include State and local jurisdictions and responder agencies, university police, and others to develop a single radio system that provides about 95 percent coverage on the State highway system. All the radios are programmed so that users reach the appropriate response agencies for various locations. The radios are easy to reprogram. The radio system also handles weather data. Police cars already are equipped with laptop computers, so when they are ready to push secure data from the TMCs, they will be able to reach law enforcement vehicles.

Emergency Management Planning

- **Iowa** integrated transportation into the emergency planning process by incorporating ESF #1 into the planning functions. For development of NIMS implementation action plans, they expanded their partner network. More than 90 counties and 500 other entities entered into the mutual aid compact.

- **Illinois** was the sixth State in the nation to receive full accreditation from the National Governors Association of its Emergency Management Program, which includes all of the agencies involved in emergency management. This is not an easy process to achieve.

- **MnDOT** developed an emergency management planning template for each of their offices and districts to complete. The template identified the incident command structure, and actions needed to set up an EOC. Annexes contain standard elements of emergency management plans.

Recovery Planning

- **Illinois DOT (IDOT)** implemented a bridge recovery plan based on both earthquake and terrorist threats. To implement the recovery plan, IDOT hired consultants who were assigned specific bridges. If something happens to the bridge, they are to report to the bridge immediately to develop a strategy for recovery.

Continuity of Operations Planning

- **WisDOT** developed a Continuity of Operations Plan that will enable them to respond to any type of incident, anywhere in the State, including a pandemic. They have a back-up site. They have co-location with the Wisconsin State Patrol (WSP) and WSP will assume the incident command function if DOT is down. The plan calls for the State Patrol to be in charge of standing up DOT's critical services.
- **Caltrans** has a business continuity plan for the entire agency, with a small chapter for each division.

Pandemic and Avian Influenza Planning

- **Minnesota** completed plans for pandemics early. The Governor participated in a facilitated tabletop exercise of the plan, as well as a DHS Assistant Secretary, and representatives of the Federal Emergency Management Agency's (FEMA's) Region 5. The exercise focused on executive-level decisions.

Evacuation Planning

- **TxDOT's** experience with Rita evacuees resulted in many lessons learned, including the critical importance of providing evacuees with expedited access to both fuel and bathroom facilities.
- In Colorado, **CDOT** is focused on evacuation plan implementation. They used traffic modeling software to plan for contraflow and evacuation by mass transit.
- **Alaska DOT** stockpiles emergency bridge replacement parts in locations throughout the State. Alaska also has done a great deal of preparation for tsunami hazards.
- New Mexico is establishing evacuation plans for the Albuquerque area, as 80 percent of the State's population is there. The **New Mexico DOT's (NMDOT's)** responsibility is to establish the evacuation routes in consideration of choke points. New Mexico hoped to do additional evacuation planning to address a potential exodus of evacuees fleeing into New Mexico due to disasters in neighboring States (or Mexico).
- Evacuation of the **Oregon** coast due to tsunami or earthquake threats is especially problematic because the east-west highways are not high-volume, and there is a relatively large seasonal tourist population on the coast. One option being considered is evacuating the coastal population to airports, and then flying the evacuees to safety. Signs have been posted that tell motorists when they are entering and leaving the tsunami evacuation area.
- **Idaho** plans for staged evacuations, where the special needs populations are evacuated first, then the general population, then the necessary providers (gas station owners, police,fire and rescue workers).

Funding

- **MoDOT** has a strong working relationship with the State Department of Homeland Security. The DOT is represented on the council that makes decisions regarding distribution of federal Homeland Security grant funds.
- **Michigan** has earmarked Federal funds to explore the application of defense technologies ("restricted use" technologies) to transportation. For example, satellites might track traffic queues across the borders to reduce travel delay, which has a major impact on manufacturing operations (and the regional and State economy).
- **Illinois DOT (IDOT)** is an active member of the Illinois Terrorism Task Force. The Task Force provides a forum for meeting, coordinating, and procuring funding.
- **Mississippi** used Federal Highway Aid money to pre-position equipment that will be needed for contraflow operations.

RESOURCES

This list of Resources was current as of the date of publication (July 30, 2009).

WEBSITES

- **AASHTO Special Committee on Transportation Security and Emergency Management.** The purpose of the Special Committee on Transportation Security and Emergency Management is to guide and support AASHTO member departments as they develop transportation security- and emergency management-related plans, policies and procedures for building and operating safe and efficient transportation networks that are resilient to threats from all hazards. The Special Committee promotes awareness and education about transportation security and emergency management among State DOTs by supporting or organizing meetings and conferences, and preparing guidance materials on a range of topics. **http://www.transportation.org/?siteid=65**

- **American Planning Association's (APA's) Policy Guide on Security.** This policy guidance was adopted by APA in 2005. **http://www.planning.org/policy/guides/adopted/security.htm**

- **FHWA Highway Infrastructure Security and Emergency Management Professional Capacity Building.** This website provides information and tools about infrastructure security and emergency management training, publications, or state contacts. Designed for highway or transportation agency employees, the site is useful for those newly assigned to positions in these functions, for research purposes, or for continuing education. Those already engaged should find this site useful as a reference repository. **http://www. fhwa.dot.gov/security/emergencymgmt/profcapacitybldg/**

- **FHWA Emergency Transportation Operations.** FHWA's Emergency Transportation Operations web page provides information about emergency transportation operations for disasters, traffic planning for Special Events (PSE) and Traffic Incident Management (TIM) programs. **http://ops.fhwa.dot.gove/eto_tim_pse/index.htm**

- **FHWA Publications Links.** The following web pages contain relevant FHWA publications.

  FHWA Operations Publications **http://ops.fhwa.dot.gov/publications/publications.htm**

  FHWA Emergency Transportation Operations Publications **http://ops.fhwa.dot.gov/publications/publications.htm#eto**

  FHWA Planned Special Events Publications **http://ops.fhwa.dot.gov/publications/publications.htm#pse**

  FHWA Traffic Incident Management Publications **http://ops.fhwa.dot.gov/publications/publications.htm#tim**

- **Lessons Learned from Information Sharing** is the national network of Lessons Learned and Best Practices for emergency response providers and homeland security officials. The website's secure, restricted-access information is designed to facilitate efforts to prevent, prepare for and respond to acts of terrorism and other incidents across all disciplines and communities throughout the United States. Access to this site is restricted to government employees (Federal, State, and local). **http://www.llis.dhs.gov/index.do**

- **National Traffic Incident Management Coalition.** The National Traffic Incident Management Coalition (NTIMC) is a unique forum where national organizations representing major stakeholders involved in traffic incident response work together. NTIMC members represent the Emergency Medical Services, Fire, Law Enforcement, Public Safety

Communications, Towing and Recovery, and Transportation communities. NTIMC promotes multidisciplinary, multijurisdictional Traffic Incident Management (TIM) programs to achieve enhanced responder safety; safe, quick traffic incident clearance; and more prompt, reliable, interoperable communications. **http://www.transportation.org/?siteid=41&pageid=590**

- **Transportation Research Board General Transportation Security.** This is TRB's leading security website. It is maintained by the Transportation Research Board (TRB) Technical Activities Division. **http://www.TRB.org/Activities/Security/TransportationSecurity1.asp**

- **TRB Recently Released Publications: Security.** To quickly locate recently released TRB publications related to security issues, go to this web page. **http://www.TRB.org/SecurityPubs**

- **TSA's Highway and Motor Carrier (HMC) Division.** TSA's Highway and Motor Carrier (HMC) Division conducts Corporate Security Reviews with highway transportation-related organizations. HMC and FEMA administer the Intercity Bus Security Grant Program and the Trucking Security Program. HMC also has programs addressing Hazardous Materials Endorsement Security Threat Assessment; School Transportation Security Awareness; Hazmat Motor Carrier Security *Self-Assessment Training; and Security Awareness outreach publications. **http://www.tsa.gov/what_we_do/tsnm/highway/index.shtm**

- **TSA Documents and Reports.** Documents, posters and brochures published by TSA's Highway and Motor Carrier Division are posted on this page. **http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm**

SECURITY INFORMATION SHARING CONTACT INFORMATION

- **Send/Receive Information with TSA Highway and Motor Carrier (HMC) Division**
  E-Mail: **highwaysecurity@dhs.gov**

- **Transportation Security Operation Center (TSOC) – Freedom Center**
  Point of Contact: TSOC Surface Watch Officer
  Telephone: 1-866-615-5150
  E-Mail: **TSOC.St@dhs.gov**

- **First Observer Program (Call Center and Highway ISAC)**
  Telephone: 1-888-217-5902
  Website: **htpp://firstobserver.com/**

- **Federal Bureau of Investigation (FBI)**
  E-Mail Tip Line: **https://tips.fbi.gov/**

TSA INITIATIVES

- **Bridge Security Pilot.** TSA is planning to work with State partners on a pilot project in which State bridge safety inspectors will compile security data on highway bridges during bi-annual bridge safety inspections. The data will be entered into the TSA's structural preparedness databases.

- **National Strategy for Highway Bridge Security.** TSA, with the DHS Offices of Policy, Science and Technology, and Infrastructure Protection; and the Federal Highway Administration, is developing a National Strategy for Highway Bridge Security, which is currently being reviewed for DHS vetting. This strategy document identifies short-, mid- and long-term approaches to enhancement of critical highway bridge security through investments of most-effective technology, structural hardening during periodic maintenance, and appropriate new structures design in the future. The strategy lays a foundation for best use of any new Homeland Security funds that may be made available to augment existing safety funds from Highway Trust Fund.

- **TSA Corporate Security Reviews.** TSA Corporate Security Reviews (CSRs) are conducted with organizations engaged in motor vehicle transportation, and those that maintain or operate key physical assets within the highway transportation community. They serve to evaluate physical and operational preparedness; to identify critical assets and key point-of-contact lists; to review emergency procedures and domain awareness training; and to provide an opportunity to share industry best practices. As of the summer of 2009, TSA had conducted 46 initial CSRs at State Departments of Transportation and three

Revisit CSRs. For more information on CSRs, contact: **highwaysecurity@dhs.gov**

- **Critical Structures Vulnerability Assessments.** TSA plans to conduct vulnerability assessments on structures identified as critical by TSA. The start date for the assessments was expected to be the fourth quarter of FY 2009. For more information on this initiative, contact: **highwaysecurity@dhs.gov**

TSA RESOURCES

- **First Observer.** "First Observer" is a national safety and security domain awareness training program that uses the skills, experiences and savvy of America's transportation professionals to help protect the critical transportation facilities and assets that move goods, services and people across America.

  First Observer is operated by Team HMS under a Cooperative Grant Agreement with the Department of Homeland Security (DHS) Trucking Security Program (TSP). The program's mission is to administer an anti-terrorism and security awareness program for highway professionals in support of the National Preparedness Guidelines. A key component of the program is to recruit volunteers from the trucking, motorcoach carrier, school bus and highway industries to act as "First Observers" in reporting suspicious activities (either criminal or potentially terrorist) to authorities. The 24/7 Call Center number is 1-888-217-5902. **http://firstobserver.com/aboutus.php**

- **HMC Government Coordinating Council (GCC)/ Sector Coordinating Council (SCC).** The objectives of the Highway GCC are 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, and between the government and private industry, in support of the nation's homeland security mission. The Highway GCC acts as the counterpart to the private-industry-led" Highway Sector Coordinating Council" (Highway SCC) for review and development of security programs necessary to protect the nation's highway and motor carrier mode. If States would like to participate, they should contact **highwaysecurity@dhs.gov**

- **HMC Regional Highway Security Exercises.** TSA's HMC plans Regional Security Exercises to discuss highway transportation security issues with security partners from the trucking, motorcoach, school transportation and infrastructure industries. These exercises as part of the Intermodal Security Training Exercise Program (I-STEP). To learn more about these exercises, or to schedule an exercise contact: **highwaysecurity@dhs.gov**

- **Security Awareness Materials.** TSA's highway-related security awareness materials cover information such as: Identifying Threats and Incidents; Recommended Procedures for Employees; Monitoring Suspicious Activities and Items; Surrounding Awareness; Collecting Information; and Responding to an Incident. **http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm**

- **Federal Security Directors (FSDs).** The Federal Security Director (FSD) is responsible for providing day-to-day operational direction for federal security at airports that have a small workforce, few checkpoints, and are directly involved in the national interest. The FSD is the ranking TSA authority responsible for the leadership and coordination of TSA security activities. These responsibilities and accompanying authority include tactical planning, execution, and operating management for coordinated security services and other duties as prescribed for the Under Secretary of Transportation for Security. The FSD is responsible for activities such as:

  - Organizing and implementing the Federal Security Crisis Management Response Plan;
  - Implementation, performance and enhancement of security and screening standards for airport employees and passengers;
  - Oversight of passenger, baggage, and air cargo security screening;
  - Airport security risk assessments;
  - Security technology implementation and maintenance within established guidelines;
  - Crisis management;
  - Data and communications network protection and recovery as it impacts on federal security responsibilities;

- Employee security awareness training;
- Supervision of Federal law enforcement activities within the purview of the FSD and TSA; and
- Coordination of federal, state, and local emergency services and law enforcement.

To locate an FSD, contact the TSA Contact Center at: **TSA-ContactCenter@dhs.gov** or call 1-866-289-9673.

- **DHS Office of Infrastructure Protection:** Protecting the nation's critical infrastructure and key resources is a key Department of Homeland Security mission established in 2002 by the National Strategy for Homeland Security and the Homeland Security Act.

  The Department's Office of Infrastructure Protection (IP) within the National Protection and Programs Directorate (NPPD) leads the coordinated national program to reduce risks to the nation's critical infrastructure and key resources posed by acts of terrorism, and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.

  For more information about the DHS Office of Infrastructure Protection, visit **http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm**

  For general questions and information regarding the U.S. department of Homeland Security, visit: www.dhs.gov. For preparedness and security information, visit **www.ready.gov**

- **Protective Security Advisors (PSAs):** PSAs are DHS' on-site critical infrastructure and vulnerability assessment specialists assigned to local communities throughout the United States. PSAs serve as DHS infrastructure protection liaisons among Federal agencies; State, local, territorial, and tribal governments; and the private sector.

  PSA Duties:

  - Perform duties as the DHS critical infrastructure protection (CIP) specialist at the State and local levels;
  - Facilitate the flow of programmatic information between DHS and parties involved in the protection of critical infrastructure;
  - Upon request, facilitate and coordinate vulnerability assessments for CIKR;
  - Assist in the confirmation of critical asset information for inclusion into infrastructure databases;
  - Support the development of the national risk picture by identifying, assessing, monitoring, and minimizing risk to critical assets at the local level;
  - Provide local context and expertise to DHS to ensure that community resources are used effectively;
  - Assist with ongoing State and local critical infrastructure security efforts, which are coordinated by the State Homeland Security Advisors (HSAs);
  - Provide feedback on the effectiveness of DHS grant funding and IP's protective programs;
  - Serve as advisors regarding infrastructure during activation of the National Response Framework;
  - Provide support during National Special Security Events and other special events, assisting with vul-

nerability assessments, security planning, and coordination; and

- Support the Joint Field Office as the Infrastructure Liaison during incidents of national significance.

PSA Program Value

- Provide guidance on established security practices.
- Support comprehensive risk analysis for local critical infrastructure.
- Convey local concerns and sensitivities to DHS.
- Assist in the review and analysis of physical/ technical security for local critical infrastructure facilities and systems.
- Communicate requests for Federal training and exercises to DHS.
- Provide communities with access to updated DHS capabilities.
- Keep communities informed of national policies related to CIKR protection.

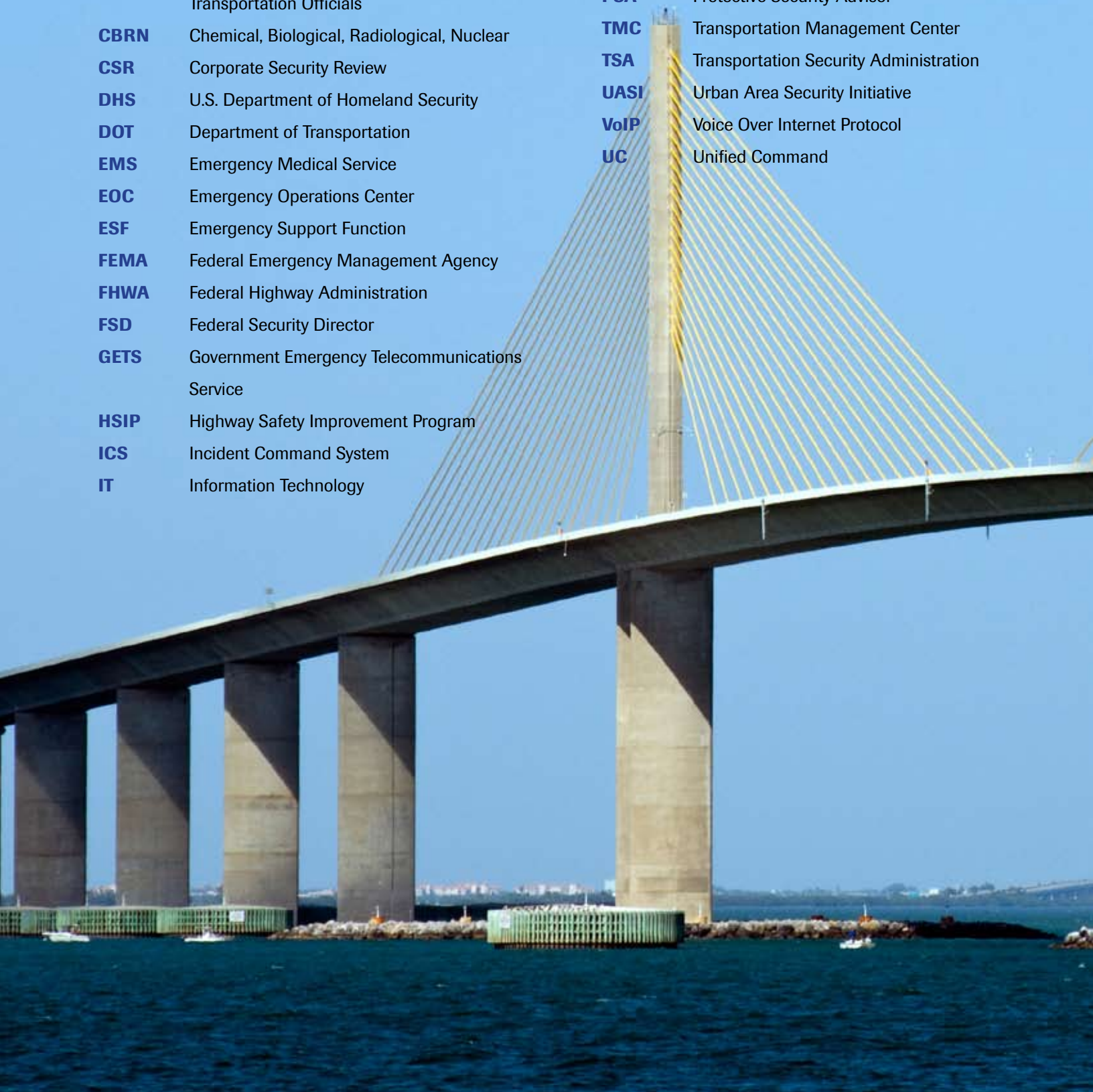
For additional information, contact your local PSA: **PSADutyDesk@hq.dhs.gov**

- **Site Assistance Visits (SAVs):** The DHS Office of Infrastructure Protection provides Site Assistance Visits as a service to stakeholders. The SAV methodology is designed to facilitate vulnerability identification and mitigation discussions between government and industry in the field. The SAV is an information gathering visit. The visit is non-regulatory and is not an inspection. There is no pass-fail grade. A report will not be sent to other agencies detailing findings from the visit. No recommendations are provided during an SAV, only options for consideration. These options are provided so that facilities may work the information into their own risk management framework to determine whether further action is merited.

  For additional information regarding SAVs and other vulnerability identification and assessment programs at DHS, contact: **jpassessments@dhs.gov**

LIST OF ACRONYMS

AASHTO	American Association of State Highway and Transportation Officials
CBRN	Chemical, Biological, Radiological, Nuclear
CSR	Corporate Security Review
DHS	U.S. Department of Homeland Security
DOT	Department of Transportation
EMS	Emergency Medical Service
EOC	Emergency Operations Center
ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FSD	Federal Security Director
GETS	Government Emergency Telecommunications Service
HSIP	Highway Safety Improvement Program
ICS	Incident Command System
IT	Information Technology
NIMS	National Incident Management System
PSA	Protective Security Advisor
TMC	Transportation Management Center
TSA	Transportation Security Administration
UASI	Urban Area Security Initiative
VoIP	Voice Over Internet Protocol
UC	Unified Command



AASHTO
THE VOICE OF TRANSPORTATION

Transportation Security Administration

U.S. Department of Transportation
Federal Highway Administration