ASSESSMENT OF HIGHWAY MODE SECURITY:
CORPORATE SECURITY REVIEW RESULTS

Highway and Motor Carrier Division
TSA Transportation Sector Network Management Office
May 2006
This Document Cleared for Public Release
The Chesapeake & Delaware Canal Bridge spans the canal near St. Georges, Delaware
Assessment of Highway Mode Security: CSR Results

Highway Transportation Overview

The highway transportation mode is unique in that it consists of privately owned vehicles traveling on publicly maintained roads. In 2001 the Bureau of Transportation Statistics (BTS) reports that the 50 states spend $104 Billion to build and maintain highway infrastructure that supported some 2.7 Trillion vehicle miles of travel.

In the US highway infrastructure includes:

- 46,717 miles of Interstate highway (BTS, 2001)
- 114,700 miles of other National Highway System roads (BTS, 2001)
- 3,801,849 miles of other roads (BTS, 2001)
- 582,000 bridges over 20 feet of span, (AASHTO, 2002)
- 54 tunnels over 500 meters in length (AASHTO, 2002)
- >50 freeway traffic operations centers (USDOT, 2002)
- >300 municipal traffic operations centers (USDOT, 2002)

The US economy is totally dependent on this infrastructure. It includes many historically and culturally significant structures that are easily accessible to vehicles of all kinds without screening or inspection. Some of these structures also have high economic value and could easily be targeted. Trucks routinely carry hazardous materials that could be used to attack targets that are part of, or are adjacent to, the highway system. This was conclusively demonstrated with a truck bomb at the Murrah Federal Building in Oklahoma City, April, 1995.

The US vehicle fleet includes 7.9 Million trucks, 750 Thousand buses, 137 Million cars, 4.9 Million motorcycles, and 84 Million other 2-axle vehicles. The motor carrier industry consists of three primary stakeholder constituencies:

The $5 Billion US Motor Coach Industry:

- Scheduled ($1.5 Billion/year),
- Charter/Tour ($3.5 Billion/year),
- 3,700 bus companies (90% are small operators with fewer than 25 buses),
- 40,000 buses,
- 190,000 jobs provided (122,000 full-time), and
- 775 million passengers annually.

The School Bus Industry:

- Largest fleet of public vehicles in the U.S.,
- 500,000 school buses,
- Transports 25 million students daily, and
- Travels 4 billion miles annually for an estimated 10 billion student trips.
The Motor Carrier Freight Industry:
  • 1.2 million motor carriers in the U.S.,
  • 9.7 million workers including 3.3 million drivers,
  • 15.5 million trucks that operate in the U.S.,
  • 40,000 new motor carriers annually,
  • 42,000 HAZMAT trucks, and
  • 75% of U.S. communities depend solely on trucking for the movement of commodities.

There is no need to further emphasize how critical motor carriers are to the economy. They constitute a particular challenge to the security community because they are not only a very distributed and independent set of potential targets but they can also be used as weapons to attack other assets that are accessible by highway infrastructure, which is most assets. Personal vehicles are of less concern to TSA so we do not plan to include these vehicles in any programs at this time.

Highway Corporate Security Reviews

Highway infrastructure reviews are a component of the TSA Highway & Motor Carrier Division’s Corporate Security Review (CSR) Program. This report covers the first two years of these reviews and is organized to correspond to TSA’s strategic objectives: Domain Awareness, Prevention/Protection, Response/Recovery, and Organizational Excellence (stakeholder service).

In May of 2004, TSA began conducting management interviews and site visits to assess the security policies and practices of organizations that operate critical highway infrastructure—such as large bridges and long tunnels, particularly those with historical significance. TSA’s corporate security reviews use a holistic approach that emphasizes the importance of management practices in prevention, protection and response for threats to the highway transportation system.

TSA is also concerned about the security of the motor carriers that convey passengers and freight on our highways. The CSR program also covers these assets and a full schedule of trucking company, motor coach operator, and school bus operator reviews is being maintained throughout 2006. Results for those parts of the CSR program will be reported in a separate document.

In the first two years of CSR operation highway infrastructure specialists in the Highway and Motor Carrier Division of have completed 36 state government reviews. These security reviews focus primarily on the state Department of Transportation (DOT) but also include other state agencies with transportation security functions. In a few cases one of these other agencies, such as the Department of Public Safety, has taken the lead. More typically, police, emergency management, and homeland security agencies were represented but principal contacts were state DOT staff.

TSA recorded information from each state reviewed in a standard set of yes/partial/no questions and in narrative form on trip reports. TSA also collected photographs and other documentation in the course of the reviews. Responses to the review questions from all the states have been entered into a spreadsheet for easier analysis. All this material has been evaluated to characterize the current state of security for highway infrastructure nationwide. This report describes what has been learned; it discusses where progress is being made and where more resources need to be applied.
Highway Infrastructure Stakeholders

The Highway and Motor Carrier Division of TSA’s Transportation Sector Network Management Office is responsible for promoting security practices for the highway mode of transportation. This includes motor carriers that carry cargo and passengers and the roads on which they travel. With the exception of PATRIOT Act requirements for hazardous materials drivers, TSA does not currently have regulations giving us legal authority over motor carriers or highway infrastructure operators. The U.S. Department of Transportation historically regulates many aspects of the highway industry, with a particular interest in promoting safety.

Counties, cities, and other local authorities own and operate most roads, bridges, tunnels and other highway facilities. Bridge and turnpike authorities operate some major facilities and there are a few privately owned bridges and roads. The average state only owns slightly less than twenty percent of the roadway miles within its borders, but this usually includes all the interstate freeways and the larger roads that are not within city limits. Typically, state-owned roads carry some three quarters of the vehicle miles traveled in the state. State governments are large, well-organized, entities that have experience dealing with federal agencies and a vested interest in securing their roadway infrastructure. As such, they were a natural starting point for TSA’s efforts to promote security through the CSR process.

State transportation agencies have long operated using an “all-hazards” approach to protecting their facilities. Many states have taken the initiative to protect their transportation assets from attack, particularly where this also reduces risk from other hazards. Although states are not receptive to the possibility of federal security regulations, particularly what they consider to be “unfunded mandates,” they are generally quite willing to consider adopting reasonable security practices. In our reviews, TSA found that many state transportation agencies have already:

- Implemented employee security awareness training,
- Conducted vulnerability assessments of bridge, tunnel and road structures, and
- Developed emergency response procedures.

These agencies know the intricacies of their structures and systems and take measures to secure their highway systems that are in accordance with what they perceive to be their risk of attack.

Stakeholder associations play a major role in communicating and coordinating security activities with TSA. State transportation agencies are represented by AASHTO through a security committee. TSA Highway and Motor Carrier Division has a liaison to this committee who regularly attends their meetings. Other associations that work with TSA are the Commercial Vehicle Safety Alliance (CVSA), the American Trucking Association (ATA), the American Association of Motor Vehicle Administrators (AAMVA), and the American Bus Association (ABA). ATA is the operator of the Highway Watch Program that includes the Highway Information Sharing and Analysis Center (ISAC). AAMVA works
Assessment of Highway Mode Security: CSR Results

with TSA on implementing PATRIOT act provisions for background checks of hazardous materials drivers and other licensing issues. CVSA partners with TSA on truck security inspections.

TSA has built a cooperative relationship with the DHS Infrastructure Protection (IP) and Grants and Training agencies, which are charged with protecting all types of infrastructure, coordinating with state and local governments, and implementing grant and training programs. Our staff coordinates with these groups on security activities to avoid duplication of effort. TSA subject matter experts have accompanied IP contractors on Site Assist Visits (SAVs) to bridges and tunnels. IP conducts SAVs on facilities in all economic sectors to better understand their vulnerability to terrorist attacks, their interdependencies with other infrastructure, and to advise their operators on how to mitigate significant problems. TSA has been inviting IP’s regionally-based Protective Security Advisors to participate in CSRs and they responded favorably.

The Federal Highway Administration (FHWA) plays an important supporting role in highway transportation security programs. There is a FHWA division office in each state and every highway infrastructure CSR has included at least one participant from this office. FHWA has also assembled a headquarters team to address security issues on federally funded highways. This team has engineers that conduct vulnerability assessments on structures and funds a number of security-related research and development projects. Our staff has worked with them on several occasions, such as a recent security review of the Golden Gate Bridge, and that cooperation continues. We are also planning to co-sponsor a series of four regional security conferences with FHWA over FY 2006 and 2007.

The Federal Motor Carrier Safety Administration’s (FMCSA) has legal authority to govern the safety of commercial motor vehicles and drivers and the safety and operations of motor carriers. FMCSA has a supporting role in commercial vehicle security, focusing their efforts primarily on the security of the hazardous materials in commercial vehicles that are under FMCSA’s jurisdiction. Specifically, HM-232 requires most hazardous materials carriers to develop and implement a security plan and conduct additional security-related training. FMCSA instituted the Security Contact Reviews (SCRs) that are targeted to carriers of hazardous materials under HM-232 to improve security preparedness, offer guidance and provide appropriate training to their field staff. TSA conducts CSRs on trucking companies with its own staff and using FMCSA-supported state inspectors in Missouri.

Corporate Security Review (CSR) Process

Selection Criteria for Security Reviews

At the beginning of the CSR program TSA selected states that were known to have well-developed security programs. This was done so TSA staff could learn what a good state highway infrastructure security program should consist of. Of course these states have well-developed programs because they have major critical infrastructure and a high level of perceived risk. Selection criteria were then broadened to include other states with highway infrastructure near the top of the DHS critical infrastructure list.

As we entered the second year of the program some low-threat states were added to provide regional balance and to explore the level of readiness outside of the high-threat urban coastal areas. We were surprised by the sophistication of the security programs in some of these states and discovered that they consider their infrastructure to be as critical as anyone’s, and for some good reasons.

Having discovered this we determined that it would be misleading to make conclusions on the country’s overall state of preparedness from a sample of a limited number of states. We also found that the contacts we gained in our state visits were a valuable contribution to the other programs our office was starting to establish. With the encouragement of AASHTO’s security committee we decided to visit all the states in
Assessment of Highway Mode Security: CSR Results

this initial sweep of security reviews. As we release this report we have visited 36 states to do security reviews and establish contacts with highway infrastructure managers. At the peak of this effort we were doing two highway infrastructure reviews a month.

New management at TSA has chosen to re-emphasize the importance of prioritizing our resource allocation based on “risk” which has lead us to reconsider the need to visit all the remaining 14 states. Plans for reviewing states that were primarily motivated by a desire to build relationships with stakeholders (in states that do not have critical transportation infrastructure) have been put on hold. Future highway security reviews are being refocused on agencies that manage highly critical infrastructure or that have experienced recent security-related highway events. Although this new emphasis has caused us to abandon last year’s goal of visiting all the 48 contiguous states by the end of calendar year 2006, it allows us to spend more time monitoring intelligence reports. So, although we may be somewhat less thorough in our stakeholder outreach we are more responsive to current events and management concerns.

The new emphasis on risk has been accompanied, coincidentally, by a reduction in the staff available to perform highway infrastructure security reviews. Both factors have functioned to reduce the rate at which our office can do these reviews. To compensate we have stepped up the number and scale of our stakeholder outreach activities. So far this year highway infrastructure has:

- Initiated a program of stakeholder conference calls
- Developed a series of four regional security conferences in conjunction with FHWA and AASHTO
- Continued our program of providing SECRET clearances to key stakeholder staff
- Offered scholarships for a few state employees to attend the Federal Law Enforcement Training Center’s five-day Land Transportation Counter-terrorism Training Program
- Attended stakeholder meetings to participate in committees and make presentations
- Started development on a secure internet “portal” on the Homeland Security Information Network for interactive discussions, sharing intelligence information, and for posting a library of resource documents

Collecting Information

TSA CSRs use a framework of 73 standard questions to interview infrastructure operators. Responses to these questions, notes made during the interview, and documents gathered during the CSR are stored in secure files at TSA headquarters and form the basis for later analysis. Any sensitive information is labeled as SSI when it is gathered at the site. Sources of information gathered during the CSRs include:

- photographs and maps of infrastructure,
- critical asset lists,
- emergency operations plans,
- training manuals,
- organizational charts, and
- vulnerability assessments.

After each CSR, TSA staff drafts a trip report that summarizes findings and captures any particularly effective security practices that were observed on the trip. This report is added to the file and forms an additional resource for analysis.
Assessment of Highway Mode Security: CSR Results

CSR interview questions are divided into eleven functional areas:

- **Threat Assessment** – 7 questions on access to, and processing of, intelligence reports on threats to the operator’s facilities;
- **Vulnerability Assessment** – 9 questions on the operator’s vulnerability assessment practices;
- **Security Planning** – 12 questions on the extent of security planning in the organization;
- **Credentialing** – 7 questions concerning organization policies on background checks and identification cards;
- **Secure Areas** – 5 questions on designation and management of controlled-access areas;
- **Critical Infrastructure** – 4 questions on how the operator determines what facilities are most critical;
- **Physical Security** – 8 questions on use of patrols, surveillance, barriers and alarms;
- **Cyber Security** – 8 questions on the use and security of computer systems;
- **Security Training** – 4 questions on the operator’s training programs;
- **Communications** – 4 questions on the operator’s practices for disseminating critical information;
- **Exercises** – 5 questions on the nature and frequency of the operator’s participation in exercises and drills.

To ensure a common approach to recording operators’ answers CSR interviewers have been trained to make consistent interpretations of operators’ responses to interview questions. TSA also developed a CSR Standard Operating Procedure document to further promote consistency.

**Analyzing Information**

TSA has developed a scoring system to help analyze operators’ responses to CSR questions. This scoring system automatically generates a numerical value to depict the relative level of security in each state. Numerical scores are used for comparative purposes and are not intended to be an absolute measure of how well an organization has implemented security practices. Figure 2 summarizes the highway infrastructure totals for the 35 states for which CSR data is available. The average score is 78 percent of the maximum possible score. The highest score was 96% and the lowest was 40%.

The states’ security scores can also be broken down by section, by question, or by arbitrary combinations of questions. This is useful for deeper analysis of the data and is illustrated in Figure 3, which shows the relative scores attained by the combined states in each of the 11 functional areas of the CSR questionnaire. It is apparent from Figure 3 that, in general, the states are not well prepared in the areas of credentialing and training.
Assessment of Highway Mode Security: CSR Results

Figure 2: Distribution of Scores for the 35 states on which CSR data is available.

Figure 3: Combined results for all states in each of the 11 functional areas.
Assessment of Highway Mode Security: CSR Results

As an example of question-level analysis, consider one of the questions TSA asks to explore practices in security training:

*Do you conduct employee refresher training on security awareness and security plan implementation?*

We record a yes/partial/no response in our spreadsheet for each state. Figure 4 shows the distribution of responses for the 35 states on which we have data.

It is important to place these responses in the context of the overall interview process. Our discussions with the infrastructure operators cover each subject in too much depth to be captured in a simple questionnaire. In this case the discussion would explore what part of the employee workforce receives refresher training, how often that training is required, how it is administered, and how extensive it is. Where the operator’s practices are particularly good or poor, TSA notes it in the trip report.

**Outreach and Partnership**

Collecting information is only one aspect of the CSR process. Our stakeholders tell us they find it particularly valuable for their organizations to get representatives of the various state agencies that perform security functions together and have this wide-ranging discussion covering all these security topics. They are also very interested in finding out what the Federal Government and the other states are doing. Establishing contacts and working relationships with state transportation security representatives is perhaps the most valuable aspect of the CSR program.

The TSA Highway and Motor Carrier Division is building a contact list of key transportation security staff in each state and has several programs designed to bring them into a national highway security community with TSA and with their counterparts in other states. These efforts include: periodic stakeholder conference calls, regional security conferences and development on a secure internet “portal” on the Homeland Security Information Network.

**Findings**

Here we report the results of our analysis of information collected from the 35 states for which highway infrastructure CSRs have been completed. Our objective was to identify issues that have influenced the ability of states to implement programs to protect their critical highway infrastructure. Where gaps are apparent we have attempted to suggest options that TSA can consider taking to help stakeholders overcome issues that may be keeping them from achieving a more effective security program. This section is organized by the four TSA strategic objectives: domain awareness, prevent/protect, respond/restore, and stakeholder preparedness (organizational effectiveness). Under each of these we have grouped the CSR subject areas that relate to that objective.
Assessment of Highway Mode Security: CSR Results

Domain Awareness

Threat Assessment
In our review of the states’ ability to receive and process information on potential threats to highway infrastructure we found that 71% of the states we visited have a means to receive, disseminate and store classified information. The majority of these states said they received threat information from external resources such as the local Joint Terrorism Task Force, FBI, Homeland Security Information System (HSIS), and Federal agencies.

Our initial interviews turned up several state DOTs that did not have staff with security clearances and sometimes did not even have access to law enforcement sensitive information. With the passage of time, it appears that designation of state Homeland Security Advisors, implementation of the Highway Information Sharing and Analysis Center (ISAC) and programs like the HSIS are giving states much better awareness of security threats. However, handling of classified information is still difficult for many transportation agencies. In general, we find that intelligence awareness is left to law enforcement agencies. The problem with this is that transportation managers don’t get an awareness of threats that comes from regularly seeing intelligence reports and so are not motivated to add security projects to their budgets.

Vulnerability Assessment
When we discussed vulnerability assessments, 74% of the states indicated that they assess their critical infrastructure. This was often just the top few critical facilities, although some states conducted, or planned to conduct, more thorough reviews of their assets. About half of the 35 states visited used the risk assessment methodology developed by the American Association of State Highway and Transportation Officials (AASHTO). Just five states preferred the Defense Department’s Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER) methodology.

The time required to perform vulnerability assessments seemed to be the main issue preventing states from assessing all their major structures. There has been some interest in TSA’s Vulnerability Self Assessment Tool (VSAT) but no states have used it so far and it is no longer being supported by TSA. Given the overwhelming preference for the AASHTO methodology we recommend that TSA continue to work with AASHTO to update their guidelines and encourage the states to them.

Infrastructure Protection (Criticality)
All but five of the states we reviewed (86%) say they have determined which of their transportation assets are critical to their operations. However, few of them have documented their criteria for doing this. On every CSR TSA staff request a list of critical highway infrastructure in that state; and on several occasions the state contact simply sat down and wrote them out from memory. The top facilities on these lists usually appear at correspondingly high positions on TSA’s list and the state representatives express a high degree of confidence in the judgment that produced the state list. This suggests that TSA should continue to integrate state inputs as part of the process of developing a national critical facilities list.

Prevent / Protect

Credentialing
All the states we interviewed issue photo identification badges to at least some of their employees. Some also provide badges for their contractors who work on state facilities. However, only 31% perform background checks on all their employees. Sixty percent do not require any kind of background checks on contractor employees, even those that work on critical infrastructure (see Figure 5). The level of
Assessment of Highway Mode Security: CSR Results

background checks ranged from a full criminal history check, to driving record and citizenship checks, down to minimal reference checks for employment applications.

Decisions about what level of background check employees need are linked with the process of identifying areas and facilities to which access must be restricted. The need for this varies from state to state, since the perceived threat and the level of risk tolerance vary from state to state. TSA has found that even prudent managers do not think it is necessary to have all their employees get full background checks.

In several cases we found that contract workers performing maintenance on critical infrastructure facilities did not have any background check at all, even though they may have been assigned to work on vulnerable areas of these structures. We recommend the use of a standard contract clause requiring such checks in these cases. TSA could draft a model clause and make it available to states for their use.

Secure Areas

The Maritime Security Act requires port facilities to formally define their secure areas. We have not found anything near this level of rigor at the states we have visited. Only half of these states (51%) have defined secure areas to the point where they can track who enters these areas and when. Even then, this designation tends to be limited to critical computer network facilities and storage areas for equipment--including explosives--in maintenance yards. It almost never extends to critical bridges or tunnels, at least not beyond the limited protection afforded by a locked gate. We found that the states’ main concerns were theft and vandalism, not prevention of terrorist attacks.

We recommend that TSA draft guidelines for the treatment of secure areas at highway facilities that take into account the variable levels of terrorist threat in different parts of the country and that leverage the “all-hazards” approach to risk that is the current accepted practice.

Physical Security

All state governments have police, highway patrol, and National Guard units at their disposal. They also have plans for emergency response and continuity of operations at some level. However, only two-thirds of the states we have visited formally define the role of these resources in preventing and responding to transportation security incidents. One reason for this is that many states do not have a staff person whose responsibility is integrating security into the planning process.

Figure 5: Number of contractors and employees get background checks.

Figure 6: State responses when asked about the use of alarms in state buildings.
Many states do not feel that there is a significant threat to their highway infrastructure. When asked if they use intrusion detection systems on their facilities (interpreted as alarms on buildings) six of the states responded that they don’t use alarm systems on any of their buildings (Figure 7). Some others only have alarms on the most critical areas. The situation with barriers (typically concrete “Jersey” barriers) was similar, with a eight of the states saying they rarely, or never, use them for security purposes.

**Cyber Security**

We found that the states we visited had many concerns, but very few actual problems with computer network security. One state reported that a faulty reserve generator switch caused their driver’s record database to be unavailable for four hours, but that was the worst of it. Many states have extensive fiber optic networks for their video surveillance systems that are used for traffic management on freeways and in tunnels, but the networks are well isolated and apparently quite robust. Traffic message signs, an attractive target for hackers on these networks, are almost never compromised.

Most states have traffic management or operations centers. Typically these are associated with large metropolitan areas. They usually have systems of video cameras focused on critical highway facilities and equipment for providing information to drivers around the state. Large bridges and tunnels usually have similar management facilities of their own. We always try to see these when we go on our facility tour after the interview. They represent a significant investment and are a critical resource for response and recovery in the case of terrorist attacks of almost any type.

We found that 60% of the states we interviewed are able to fully restore operations center functions at a backup location should their primary center become incapacitated. Given the growing importance of these centers, it would be good for states without this capability either develop an alternate location or enhance the survivability of the location they have.

**Respond / Restore**

**Communications**

The states have noted at various meetings and conferences that they have worked hard to implement strong communication systems to help them respond effectively to incidents. Our CSR findings show implementation rates of around 90% for the capabilities we ask about. Discussions show that interoperability problems between police and transportation department radio systems have been largely resolved but that problems communicating with fire departments continue.

In general, state organizations know who to contact in an emergency. They have backup means of communication should their primary means fail, and they have plans to contact federal agencies when necessary. They usually have “courtesy patrols” and maintenance trucks that have radio contact with a dispatcher and have cell phones as backup.

---

1 In several states we observed that it was possible to drive a truck right up to within a few feet of the state capitol.
All the states participate in the “Amber Alert” program and have some traveler information capabilities (511 telephone, message signs, highway advisory radio, and/or web sites). They have plans to use these for emergency response and evacuations but rarely for security incidents.

**Exercises**

A high percentage of states periodically conduct exercises and drills. In a number of states transportation personnel indicated that they participate but don’t initiate or lead because they see their role as providing a service to the emergency management, or other, first responder agency.

Transportation agency staff are not considered to be “first responders” by Federal or state agencies. In this they typically defer to the Department of Public Safety or to the local fire department as mandated by the Emergency Management System (EMS). They are, however, often called upon to provide services early in the development of an emergency situation. They seem to be prepared to do this under normal circumstances but, as recent exercises have demonstrated, issues can arise in terrorist attacks for which they are completely unprepared.

Since transportation agencies are not first responders, they are also not eligible for DHS first responder grant funds. They would very much like to be able to present their projects for this funding. Broadening the definition of “first responder” to include certain transportation agency functions would address this need and would give DHS a better selection of proposals for this important program.

**Stakeholder Service**

**Security Planning**

86% of states reported that they conduct security planning at the state level. State governments vary considerably in the way they are organized. States assign different security functions to different agencies—particularly for transportation security functions. Each agency does some level of planning to ensure its ability to perform its functions. These preparations are documented in many places, such as: emergency response plans, traffic management plans, hazmat management plans, National Guard plans, Homeland Security Advisory level preparedness plans, Continuity of Operations plans, and police patrol plans. Some are more complete than others, depending on the diligence of the agency.

However, when asked if they have a “security plan” such as the one described in the Maritime Security Act, only two thirds (63%) of the states could meet our criteria for saying yes. We gave them credit if they had a document that defined basic responses to different threat levels and defined who was in charge (a security officer). The states that had a plan and a security officer also tended to periodically review their plan and usually had executive-level support.

One issue is that few states have a dedicated budget for transportation security (Figure 8). If security rises to the level of a program with a budget then planning naturally follows. If it is just a few projects cobbled together from the maintenance budget then it tends not to receive the same level of support.

![Figure 8: Does the state have a dedicated budget for transportation security?](image)
Assessment of Highway Mode Security: CSR Results

Training
Of the states reviewed, 71% said they had conducted employee security awareness training. When questioned further this was often a one-time response to the September 11 attack. Only half said they conducted refresher training (at any level of frequency) and just 40% had documented their training program. Our conclusion is that much more could be done here.

State transportation agencies have active training programs. Security awareness training programs are inexpensive, readily available, and only require an hour or two for each employee. It should be required that the employee refresh his knowledge by retaking the course every year or two. Security training can easily be combined with periodic training required for safety and other purposes.

TSA could encourage the states to add security awareness to their required training programs by making an appropriate training program available (NTI an Highway Watch training programs are likely candidates) and by providing delivery guidelines.

Conclusions

Management Challenges
After two years of operations the highway infrastructure security review program has evolved into a nearly mature process. TSA’s philosophy has been to maintain flexibility and adapt to management direction and the changing interests of the stakeholder population. We have learned a great deal about what both our management and our stakeholders expect. We have grown into a role of communicating these expectations and facilitating the development of programs to provide for the needs of both groups.

The CSR program is intended to perform three separate functions:

• Build a working relationship with stakeholders,
• Provide security program advice and technical expertise, and
• Collect data to quantify the state of security in the industry.

This year TSA’s trucking and motorcoach teams have stared performing security reviews at organizations that operate motor carrier and school bus fleets. The infrastructure team has reviewed two bridge authorities and has done reviews in conjunction with FHWA and TSA’s Risk Office. Experience with diverse stakeholders will help further identify management issues.

Filling Gaps, the Path Forward

Findings from the CSRs that have been performed with state highway infrastructure operators over the first year of the program suggest a number of security management areas that could benefit from additional resources. Recognizing that TSA is not likely to be able to provide direct funding to these entities there are still ways we can help our stakeholders protect their critical infrastructure. Here are some steps TSA can take to achieve these ends:

• Perform CSRs in all the remaining states to promote stakeholder outreach (even where the risk is minimal local organizations feel that their infrastructure is important and we can’t forget that Oaklohoma City is a low-risk area).
• Continue to extend the CSR program to bus and truck operators.
Assessment of Highway Mode Security: CSR Results

- Work with AASHTO to put on regional conferences for stakeholders to share best practices and distribute the proceedings of these conferences as a resource.

- Develop a model clause to include in contract requirements for work on critical infrastructure that describes which contract workers need to have what level of background checks.

- Produce a set of “performance-based” objectives that agencies can use to evaluate and plan their programs.

- Help states without backup capability at traffic operations centers develop an alternate location or enhance the survivability of their single location.

- Encourage DHS to broaden the definition of “first responder” to include certain transportation agency functions to give them access to DHS grant programs.

- Help the states to add security awareness to their required training programs by making an appropriate training program available.

- Facilitate the development of a “culture of security” by fostering the sense of everyone having a part and by providing a web site for discussions and resources.

TSA staff under West Virginia’s New River Gorge Bridge, 700 feet above the river
For Information or to Request a CSR Contact:

Bill Arrington  
General Manager  
Highway and Motor Carrier Office  
Transportation Security Administration  
TSA-28, 601 S 12th St., Arlington VA 22202  
571-227-1500  
highwaysecurity@dhs.gov