Rail Security for Passenger Rail
David Armour – Los Alamos Technical Associates Inc.

Rail Transit Security - Background

Communities across the United States rely on reliable, safe, and secure rail systems. Each weekday, more than 12 million passengers take to U.S. railways. Recent attacks on passenger-rail systems around the world highlight the vulnerability of this form of transportation. The high use of passenger rail and the frequency with which terrorists target rail systems elsewhere call for a commitment to analyzing and improving rail security in the United States.

The goal of this presentation is to assist Transit Agencies in the development of a framework for security planners and policymakers that can be used to guide cost-effective rail security planning.

Transit Security Risk

The security concerns pertinent to a Transit Agency address the risk of terrorism to a degree, but Transit Agencies put a greater emphasis is on the risks associated with transit crime and liability prevention.

As regards this presentation, risk is a function of:

- **Threat**
  - Presence of terrorists with intent, weapons, and capability to attack
  - Presence of criminal activities (violent crime, theft or robbery, vandalism)
  - Presence of budgetary loss through legal liability or inability to successfully prosecute criminals.

- **Vulnerability**
  - Terrorist attack - likelihood of damage at a target, given an attack
  - Criminal act – likelihood of passenger harm, loss of assets, legal liability or inability to successfully prosecute criminals

- **Consequences**
  - Terrorist attack - nature and scale of damage if an attack succeeds
  - Criminal act – nature and scale of damage if a criminal act succeeds
  - Liability – nature and scale of monetary accountability of the Agency if there is no evidence to refute/mitigate claim

While effective security solutions may address all three components of risk for both terrorist and criminal acts, this presentation focuses on addressing vulnerabilities and limiting consequences, since these are the two components of risk most within the realm or under control of Agency rail-security personnel.
This presentation includes security considerations based on both Rail Terrorism and Transit Crime. Two studies were used as primary reference, as follows:

- Regarding Terrorist Activities, a study performed by RAND specifically for the Department of Homeland Security is used as reference, which is focused on passenger, as opposed to freight, rail systems. Because of the tremendous variation in the types of rail systems and the desire not to reveal the specific security measures of any one rail system, the RAND analysis was based on a hypothetical model rail system that characterizes rail systems typically found in the United States.
- Regarding Transit Crime, the Federal Transit Administration’s 2004 study on Transit Crime provided the reference for criminal statistics focused on Passenger Rail contained in this presentation.

**Terrorist Rail-Attack Threats**

Drawing primarily on available data on past terrorist attacks on rail systems from the RAND-MIPT Terrorism Incident Database (National Memorial Institute for the Prevention of Terrorism and RAND Corporation, ongoing), we found that:

- the most prevalent terrorist threat to rail systems comes from bombings,
- that most terrorist attacks on rail systems produce few fatalities and injuries, and
- that attacks in densely packed rail cars and interior rail-facility locations are of particular concern because of the casualties they can produce.

Not all terrorist attacks on rail systems come from explosives, so security measures must address explosive devices but also appropriately incorporate the possibility of rarer attack modes. In addition, given the damage associated with a relatively small number of large attacks, security measures that prevent only the largest-scale attacks could significantly reduce the human costs associated with this threat.

Although historical data and the patterns of behavior they document provide a foundation for security decision making today, it must be emphasized that terrorists are dynamic adversaries whose attack patterns may change in response to security measures. Security portfolios of Transit Agencies, thus, should not be static defenses, but rather should be reviewed periodically to ensure that they remain relevant to any changes in terrorists’ targeting methods.

**Passenger Rail and Terrorism Risk**

To understand the vulnerability of rail systems to the terrorist threat, we constructed a hypothetical rail system. We then subjected that notional system to a range of attack scenarios to identify the specific set of attacks to which the rail system was most at risk.

The threat scenarios were drawn from past attack reports and other open-source information.
The vulnerability assessment identified 11 potential target locations (e.g., system operation and power infrastructure) within a notional rail system and eight potential attack modes (e.g., small explosives). These targets and attack modes were combined to produce 88 different attack scenarios of concern. Each scenario was then categorized high, medium, low, or no risk. The categorization represents qualitative judgments about terrorists’ ability to exploit the vulnerability and the consequences if they were to succeed, as shown below.

### Table 2.1

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Armed attack</td>
<td>55</td>
<td>6</td>
</tr>
<tr>
<td>Arson</td>
<td>29</td>
<td>3</td>
</tr>
<tr>
<td>Barricade or hostage</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Bombing</td>
<td>708</td>
<td>80</td>
</tr>
<tr>
<td>Hijacking</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Kidnapping</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Sabotage</td>
<td>49</td>
<td>6</td>
</tr>
<tr>
<td>Unconventional attack</td>
<td>24</td>
<td>3</td>
</tr>
<tr>
<td>Unknown</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>Logistics activity (nonattack)</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>886</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

**Criminal Rail Threats**

Drawing primarily on available data on criminal activities on rail systems from the Federal Transit Administration’s 2004 study on Transit crime, it was found that Light Rail is far more susceptible to crime than buses.

Regarding violent crime, National Federal Transit Administration data for 2004 indicate that, per passenger mile, light rail is involved with more than 3 times as many aggravated assaults, 26 times as many burglaries, 7 times as many rapes, and 10 times as many robberies as buses. The numbers for 2005 and 2006 are similar.

One reason why buses are safer from violent crime is that the bus driver is in the same compartment as the passengers and acts as a moderating influence on passenger behavior. Light-rail drivers have their own secure compartments safe from passengers trying to hijack their trains, ask for directions, or get help from muggers. In multi-car consists, the driver is often not in the same car as the violent criminal. While the driver is protected, riders are less so.

Light rail is also associated with near vicinity property crime near rail stations. The chief of police in one of Portland’s suburbs told me that they are very aware that, every time a
new light-rail station opens, burglaries, vandalism, and similar crimes increase in that neighborhood.

A key reason is that transit agencies run rail lines far more frequently than buses, and that frequency provides criminals a fast ride away from the scene of their activities.

This fact naturally elevates the prevention of criminal activities on rail into the highest priority status, and in terms of metropolitan light rail, the open communications, cooperation and system alarm linkage with local law enforcement attains paramount importance.

Along with property and theft crimes, the incidence of violent crime in metropolitan light rail is also of import.

Of crime on rail, the following facts are brought forth by the FRA study.

<table>
<thead>
<tr>
<th>Weapon</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explosives</td>
<td>643</td>
<td>77</td>
</tr>
<tr>
<td>Fire or firebomb</td>
<td>39</td>
<td>5</td>
</tr>
<tr>
<td>Firearms</td>
<td>51</td>
<td>6</td>
</tr>
<tr>
<td>Chemical agent</td>
<td>17</td>
<td>2</td>
</tr>
<tr>
<td>Radiological agent</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Threat</td>
<td>65</td>
<td>8</td>
</tr>
<tr>
<td>Unknown</td>
<td>18</td>
<td>2</td>
</tr>
<tr>
<td>None</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>837</td>
<td>100</td>
</tr>
</tbody>
</table>

SOURCES: Analysis of rail incident data compiled from National Memorial Institute for the Prevention of Terrorism and RAND Corporation (ongoing), Jenkins (1997, 2001), Rabkin et al. (2004), and Monterey Institute of International Studies (undated[b]).

* This total reflects that sabotage incidents were not assigned a weapon type. There were 49 sabotage incidents (see Table 2.1), and 886 – 49 = 837.

Transit Priority to Prevent Liability Loss Though Evidentiary Security Data Collection

As we have learned in developing security solutions for Transit Agencies, in addition of Terrorist and Criminal Security, a key priority in security system requirements is the inclusion of security technology elements that mitigate liability and reduce potential loss through a variety of unsubstantial claims that may be made by ridership.
All rail systems have at least some security measures in place that provide evidentiary safeguards to refute frivolous lawsuits and demonstrate no fault of the Agency in such claims.

**Baseline Security and Operational Characteristics of the Passenger Rail System Model as Applicable to Transit Agencies**

The end objective is to identify *additional increments* to security that can be implemented in a cost-effective manner. However, all rail systems have at least some security measures in place, and those security measures, in turn, have some impact. Thus, the study had to further specify our notional rail system by describing the existing baseline security system and its effectiveness.

The study assumed a relatively simple notional rail network located within a major metropolitan area, consisting of five spokes of unique rail lines going directly into one hub central station, with the only transfer point between these lines located at the hub station.

The study further assumed that the baseline notional rail-security system would have the following security measures in place: perimeter and station surveillance systems, uniformed patrols, available rapid-deployment forces, and an automated vehicle locator (AVL) system (assumed to be located at the operation-control center) for detecting unusual delays in trains within any one of the many lines within the notional rail system.

In addition, the study adopted the vision of a multilayered transportation security system illustrated in a recent Federal Transit Administration report (Rabkin et al., 2004), in which we defined each layer as going from first safeguarding the outermost *perimeter* to the *exterior, interior, and restricted access* areas to the innermost rail security *asset*, the trains.

**Cost-Effective Security-Improvement Options for the Notional Rail System**

With the notional system’s existing security defined, we could then turn our attention to what improvements to that security could be made. We identified 17 security-improvement options (SIOs) within three broad categories:

1. process-based improvements (e.g., implementing enhanced security training),
2. technology-based alternatives (e.g., using portable [handheld] detection systems), and
3. infrastructure and facility modifications (e.g., installing blast-resistant containers).

The study assessed the relative effectiveness of the 17 SIOs across the five security layers laid out above. We evaluate effectiveness by assessing the SIO’s performance against four criteria:

1. preventing or reducing the probability of a specific terrorist attack occurring,
2. reducing or averting the number of fatalities of passengers in the system,
3. reducing the time necessary for system facilities and infrastructure to be restored and operations fully resumed, and
4. minimizing rail operating revenue losses.

The 17 security measures were rated for their incremental impact at each layer, as well as to their potential system-level contribution across layers.

At the system level (integrating across layers), we identified four broad categories of cost-effective security measures for system operators to consider:

1. relatively inexpensive solutions with the highest effectiveness-per-dollar metric payoffs (e.g., enhanced security training),
2. additional inexpensive solutions to consider with reasonable levels of effectiveness-per-dollar metric payoffs (e.g., installing retractable bollards at entrances and exits of the operation-control center and power plant),
3. costlier solutions with highest effectiveness-per-dollar metric payoffs (e.g., installing fixed barriers at curbsides adjacent to all entrances and passageways leading to ground-level and underground stations), and
4. relatively expensive, longer-term solutions for future consideration (e.g., rail-vehicle surveillance systems).

For our notional system, even though we prioritized the mix of security measures relative to affordability, the actual list of recommendations could depend on a variety of practical constraints, concerns, or needs, such as the ease and speed of implementation or budget constraints relative to other rail-system expansion plans.
Rail-Security Policy Considerations

Given the open and accessible characteristics of rail systems, the unpredictability of terrorist attacks, the continual evolution of risk as terrorists learn and improve their capabilities, and finite resources for security provision, the United States faces a complex security problem that has existed for decades.

This approach illustrates a process—a framework and a broad range of management considerations—for thinking through how to systematically improve the security of U.S. passenger systems to help ensure maximum protection at the lowest cost.

Rail-Security Lessons at the System Level

Security planners can draw from the FRA Security Planning framework and optimize security-improvement efforts. The process begins with conducting a detailed vulnerability assessment. Once the system’s vulnerabilities are understood, potential increments or additions to existing security measures can be identified.

As the security posture of a specific rail system is examined, two factors must be kept in mind. First, security measures designed to thwart terrorism may have an added impact on preventing and mitigating ordinary crime or may have to be scaled up to address crime-related issues.

Thus, the security measures chosen may have broader costs and benefits than those relating only to terrorism. Second, terrorists may seek to overcome defensive measures. Thus, those in charge of acquiring security improvements must consider how terrorist groups might react to potential security improvement defenses put in place, so that they can make informed investment decisions.

The Future of Rail Security

We have already witnessed some important changes in terrorist-attack patterns against transportation in the few short years since 9/11, including concerted efforts to develop bombs that can evade airport detection equipment.

Thus, we can predict with near certainty that terrorist-attack patterns will change in the future, though we cannot predict with much certainty precisely how those changes will be manifested.

Given this uncertainty, rail-security systems must be designed to be responsive to potential changes in attack patterns, and the consequent impact on the relative effectiveness of the security portfolio must be reevaluated periodically.

Research and development in improving and maturing countermeasure technologies and investments in human capital are elements of developing and maintaining robust security measures. Improvements in the performance of these technologies can
diminish the terrorists’ ability to successfully attack and reduce the indirect costs of security operations, such as the time required to screen passengers and baggage. Though technologies can perform many security functions, the people who use and monitor them are frequently the most critical element of the overall security system, and there is no substitute for having highly responsive and skilled staff in the security loop.

To maintain the performance of personnel at the highest readiness levels, managers will have to invest in both enhanced security training and field testing. The former ensures that the personnel are most adept at operating the latest technologies; the latter helps ensure that they are highly proficient in implementing the set of emergency-response protocols and procedures as needed.

**Rail Security versus the Security of Everything Else**

A common response by terrorists to the deployment of security measures is simply to move attack operations away from the defended area to softer targets located elsewhere.

If defenses are deployed in one rail system, this behavior could move risk from one site to another. Likewise, if rail-security measures are increased across the entire rail transportation system, attacks may simply be displaced onto other targets, such as a shopping mall or sport stadium. Under some circumstances, displacement could be viewed as a favorable outcome, if, for example, the attack was displaced to a location that is much easier to respond to than the original target location would have been.

Given that security in one setting relates to security in another, federal policymakers ultimately must decide how best to allocate security dollars not only across rail systems but also across other modes of transportation, critical infrastructure, and public venues.

We cannot, from this analysis, draw conclusions about whether authorities should spend more on rail and less on air-transportation security, because we did not conduct such cross-mode and cross-target comparisons. We can, however, point to the applicability of this assessment methodology to decision making about allocating security resources generally. We strongly encourage analysts, scholars, and researchers to extend the application of this form of methodology to such critical resource allocation problems.

**Conclusions**

It bears repeating that the prioritized SIOs identified by following Security Planning guidelines are specific to the notional system, which can be used as an example and strawman for building in the specific requirements and priorities of each rail operator.

The methodology presented in the FRA Security Planning guideline is useful for planning rail-security options. The methodology should, however, be tested against other security planning systems of varying complexity. Such testing will yield two
insights. First, we will understand better whether the portfolio of preferred SIOs varies with system complexity or is largely the same regardless.

Since both risk and the nature of preexisting security measures will vary by the type of system examined, such experimentation will also give some insight into the dynamic nature of the threat- and security-assessment processes and, perhaps, the timeline over which the assessments need to be repeated to counter the fact that terrorists wield new methods and learn potential targets’ defenses over time.

Second, applying the methodology to systems of differing complexity will allow us to better understand the information demands that the framework imposes. The methodology is most useful if the information it requires is relatively easily obtained in a consistent and comprehensive manner.
Rail Security – Integration of DHS Security Agenda with Transit/Transportation Priorities

David Armour

Los Alamos Technical Associates, Inc.
Each weekday, more than 12 million passengers take to U.S. railways. Recent attacks on passenger-rail systems around the world highlight the vulnerability of this form of transportation.

The high use of passenger rail and the frequency with which terrorists target rail systems elsewhere call for a commitment to analyzing and improving rail security in the United States.
Transit Security Risk

The security concerns pertinent to a Transit Agency address:

- Terrorism
- Transit Crime
- Liability Prevention and Mitigation
Transit Security Risk

As regards this presentation, risk is a function of:

- **Threat**
  - Presence of terrorists with intent, weapons, and capability to attack
  - Presence of criminal activities (violent crime, theft or robbery, vandalism)
  - Presence of budgetary loss through legal liability or inability to successfully prosecute criminals.

- **Vulnerability**
  - Terrorist attack - likelihood of damage at a target, given an attack
  - Criminal act – likelihood of passenger harm, loss of assets, legal liability or inability to successfully prosecute criminals

- **Consequences**
  - Terrorist attack - nature and scale of damage if an attack succeeds
  - Criminal act – nature and scale of damage if a criminal act succeeds
  - Liability – nature and scale of monetary accountability of the Agency if there is no evidence to refute/mitigate claim
References

This presentation is based on two studies:

- **Terrorism** - The RAND Study for the Department of Homeland Security
  - Focused on passenger, as opposed to freight, rail systems.
  - Because of the tremendous variation in the types of rail systems and the desire not to reveal the specific security measures of any one rail system, the RAND analysis was based on a hypothetical model rail system that characterizes rail systems typically found in the United States.

- **Crime** – The Federal Transit Administration’s 2004-2006 study on Transit crime
  - Focused on Passenger Rail.
  - Included violent crime (rape, assault, bodily harm), property crime and theft.
Terrorist Rail-Attack Threats

Drawing primarily on available data on past terrorist attacks on rail systems from the RAND-MIPT Terrorism Incident Database (National Memorial Institute for the Prevention of Terrorism and RAND Corporation, ongoing), we found that:

• The most prevalent terrorist threat to rail systems comes from bombings,
• That most terrorist attacks on rail systems produce few fatalities and injuries, and
• That attacks in densely packed rail cars and interior rail-facility locations are of particular concern because of the casualties they can produce.
Terrorist Rail-Attack Threats

The vulnerability assessment in the Rand Study identified:

- 11 potential target locations (e.g., system operation and power infrastructure) within a rail system.
- 8 potential attack modes (e.g., small explosives).
- These targets and attack modes were combined to produce 88 different attack scenarios of concern.
- Each scenario was then categorized high, medium, low, or no risk.
## Terrorist Rail-Attack Tactics

### Table 2.1: Terrorist Tactics in Rail Incidents

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Armed attack</td>
<td>55</td>
<td>6</td>
</tr>
<tr>
<td>Arson</td>
<td>29</td>
<td>3</td>
</tr>
<tr>
<td>Barricade or hostage</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Bombing</td>
<td>708</td>
<td>80</td>
</tr>
<tr>
<td>Hijacking</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Kidnapping</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Sabotage</td>
<td>49</td>
<td>6</td>
</tr>
<tr>
<td>Unconventional attack</td>
<td>24</td>
<td>3</td>
</tr>
<tr>
<td>Unknown</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>Logistics activity (nonattack)</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>886</td>
<td>100</td>
</tr>
</tbody>
</table>
## Terrorist Rail-Attack Weapons

### Table 2.2
Weapons Used in Rail Incidents

<table>
<thead>
<tr>
<th>Weapon</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explosives</td>
<td>643</td>
<td>77</td>
</tr>
<tr>
<td>Fire or firebomb</td>
<td>39</td>
<td>5</td>
</tr>
<tr>
<td>Firearms</td>
<td>51</td>
<td>6</td>
</tr>
<tr>
<td>Chemical agent</td>
<td>17</td>
<td>2</td>
</tr>
<tr>
<td>Radiological agent</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Threat</td>
<td>65</td>
<td>8</td>
</tr>
<tr>
<td>Unknown</td>
<td>18</td>
<td>2</td>
</tr>
<tr>
<td>None</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>837</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

**Sources:** Analysis of rail incident data compiled from National Memorial Institute for the Prevention of Terrorism and RAND Corporation (ongoing), Jenkins (1997, 2001), Rabkin et al. (2004), and Monterey Institute of International Studies (undated[b]).

*This total reflects that sabotage incidents were not assigned a weapon type. There were 49 sabotage incidents (see Table 2.1), and 886 – 49 = 837.*
Criminal Rail Threats

Drawing primarily on available data on criminal activities on rail systems from the Federal Transit Administration’s 2004-06 study on Transit Crime, it was found that Light Rail is far more susceptible to crime than buses.
Criminal Rail Threats

- Regarding violent crime, per passenger mile, light rail is involved with more than:
  - 3 times as many aggravated assaults,
  - 26 times as many burglaries,
  - 7 times as many rapes, and
  - 10 times as many robberies as buses.
Buses are safer than light rail because:

- The bus driver is in the same compartment as the passengers and acts as a moderating influence on passenger behavior.
- Light-rail drivers have their own secure compartments safe from passengers trying to hijack their trains.
  - In multi-car consists, the driver is often not in the same car as the violent criminal. While the driver is protected, riders are less so.
Criminal Rail Threats

Buses are safer than light rail because:

• Light rail is also associated with near vicinity property crime near rail stations.
  – The chief of police in one of Portland’s suburbs told me that they are very aware that, every time a new light-rail station opens, burglaries, vandalism, and similar crimes increase in that neighborhood.

• Transit agencies run rail lines far more frequently than buses, and that frequency provides criminals a fast ride away from the scene of their activities.
Liability and Fraud Prevention

It is a Transit Agency Priority to Prevent Liability Loss Though Evidentiary Security Data Collection

- In addition of Terrorist and Criminal Security, a key priority in security system requirements is the inclusion of security technology elements that mitigate liability and reduce potential loss through a variety of unsubstantial claims that may be made by ridership
Liability and Fraud Prevention

- All rail systems have at least some security measures in place that provide evidentiary safeguards to refute frivolous lawsuits and demonstrate no fault of the Agency in such claims.
- Video Surveillance is the Key Liability Prevention Tool for Transit Agencies
Transit Agency Planning and Requirements

- The predecessor to Security Funding is Comprehensive Transit Agency Security Planning
- This includes the analyses required for DHS Allocations and other Federal Grants
- The primary priorities of DHS are not in the same order as the priorities of Transit in terms of Agency budget
- The challenge is to develop a Security Strategy that supports both DHS and Transit security objectives with a limited yearly Agency security budget.
Transit Agency Planning and Requirements

• Federal Transportation Administration document FTA-MA-90-7001-94-1 provides a comprehensive guide in the formation of a Transit Security Plan.

• However, it relies on the knowledge of the Transit Agency in identifying, assessing and prioritizing risks.

• Each Transit Agency has vastly different issues, constraints and requirements for Security.
Transit Agency Planning and Requirements

- Based on findings of analysis performed during Planning, identify all areas where risks and vulnerabilities are greatest.
- Develop concepts for mitigation of vulnerabilities, beginning with highest priorities.
- Of high priority items, identify all mitigation concepts/strategies that mitigate both DHS and Transit Security issues (overlapping or multi-faceted positive impact).
Overlapping Impacts

• These overlapping impacts allow the Agency to identify which high priority mitigation concept to implement first.
  – e.g. Video Surveillance mitigates DHS concerns (terrorist) as well as Transit concerns (crime and liability)

• As the Agency develops the Security Plan, the groundwork is laid for application to a number of Federal Security Grants
Transit Agency Grant Specific Legacy Options

- Research and prepare all applicable grants and Federal funding programs relevant to Security. These include:
  - **Preparedness Grants** (non-disaster)
    - Emergency Management Performance (EMPG)
    - Emergency Operations Center (EOC)
    - Homeland Security Grant (HSGP)
      - State Homeland Security Grant (SHSP)
    - Freight Rail Security (FRSP)
    - Intercity Bus Security (IBSGP)
    - Intercity Passenger Rail Security (IPR)
    - Transit Security Grant (TSGP)
    - Security Continuing Training Grant
    - Emergency Operations Center Grant Program
  - **Disaster Grants**
    - FEMA
    - Federal Disaster Assistance

- NOTE: Completing the Security Plan and Requirements provides the groundwork and input for developing the Grant Requests.
Transit Agency Grant Other 2012 Programs

Homeland Security Grant Program (HSGP)—provides more than $830 million for states and urban areas to prevent, protect against, mitigate, respond to, and recover from acts of terrorism and other threats.

- **State Homeland Security Program (SHSP)**—provides $294 million to support the implementation of state homeland security strategies to build and strengthen preparedness capabilities at all levels. The 9/11 Act requires states to dedicate 25 percent of SHSP funds to law enforcement terrorism prevention activities.

- **Urban Areas Security Initiative (UASI)**—provides more than $490 million to enhance regional preparedness and capabilities in 31 high-threat, high-density areas. The 9/11 Act requires states to dedicate 25 percent of UASI funds to law enforcement terrorism prevention activities.

- **Operation Stonegarden (OPSG)**—provides more than $46 million to enhance cooperation and coordination among federal, state, territorial, tribal and local law enforcement agencies to jointly enhance security along the United States land and water borders.

- **Urban Area Security Initiative**—Can be used by Transit Agency serving a large metropolitan area.
SUMMARY

- Transit and DHS priorities for rail are similar, but separate.
- There are numerous avenues for appropriating Federal funding for Transit projects and programs that are security driven.
- The key to gaining Federal funding via grants is proper security planning and the inclusion of capabilities that meet both Transit and DHS requirements.
- The Grant programs change yearly. New grants and the extension of existing grants make keeping up with what is available each fiscal year a necessity.