5.9 MULTI-MODAL SECURITY

INTRODUCTION

The federal government in 1998, called for states and MPOs to address transportation security issues. In 2005, a new transportation act strengthened the requirement, which has been extended to the current FAST Act. The transportation acts require long-range regional transportation plans to consider security distinct from transportation safety. Furthermore, in 2002 the Transportation Security Administration (TSA) was created with extensive requirements for operational and capital improvements relating to security. While the public's eye has been on passenger aviation, TSA's mission relates to all modes.

The federal government anticipates that over the next several years, security considerations will result in changes in how transportation is planned, designed, implemented and operated. Transportation goals, planning processes, databases, analytical tools, decision-making considerations, and organizational structures will change due to security concerns. Transportation will be on the front line in responding to security risks. The response to security concerns will be cross-jurisdictional and functional lines and be among the most complex and important challenges to transportation professionals. While it may be too early to begin changing our long-range infrastructure network plans in response to security risks, there will be changes in spending priorities in the near term and most probably over a longer period of time.

There is a wide range of incidents that could cause varying levels of disruption to the transportation system. One report recommending a national research and development strategy for improving surface transportation security presented a wide ranging list of possible threat scenarios. The list originated in a U.S. Department of Transportation vulnerability assessment of the U.S. transportation system. The nature of the threats was characterized primarily as being a physical, biological, chemical or cyber-attack. The types of responses would clearly be different depending on the nature of the attack.

The magnitude and scope of an incident will clearly be an important determinant for gauging the appropriate public safety/emergency response. And most studies of sudden disruptions to the transportation network, either from natural or man-made causes, have concluded that the redundancies in a metropolitan area's transportation system provides a rerouting capability that allows the flow of people and vehicles around disrupted network links. For instance, in the RVMPO area, parallel north-south routes Hwy 99 and I-5 offer that redundancy.

DEFINITIONS

The simplest distinction between safety and security is that safety problems- accidents – are just that—unpremeditated unfortunate events. As such, they may be caused by driver error or impairment, adverse weather, a temporary hazard in the

right-of-way, poor infrastructure or vehicle design, or all of the above. By contrast, security events always connote a negative intention, whether the perpetrator is a disgruntled single individual, a member of a gang, or a member of a political organization, that is, a terrorist. In number, terrorist attacks on transportation systems are few, with the vast majority of security breaches being perpetrated by non-political actors. But terrorist events, when they do occur, can be much more dramatic, harm many more people, and require much more to address. The following table provides a description of various types of security problems that can arise in any transportation system.

Table 5.9.1: Examples of Transportation Security Incidents

Event	Description
Aggravated Assault	An unlawful attack by 1 person upon another for the purpose of inflicting severe or aggravated bodily injury. This type of assault usually is accompanied by the use of a weapon or by means likely to produce death or great bodily harm.
Arson	To unlawfully and intentionally damage, or attempt to damage, any real or personal property by fire or incendiary device.
Burglary	The unlawful entry of a structure to commit a felony or a theft. This includes offenses known locally as burglary (any degree), unlawful entry with intent to commit a larceny or felony, breaking and entering with intent to commit a larceny, housebreaking, safe cracking and all attempts at these offenses.
Larceny/Theft	The unlawful taking, carrying, leading or riding away of property from the possession or constructive possession of another. This includes pocket picking, purse snatching, shoplifting, thefts from motor vehicles, thefts of motor vehicle parts and accessories, theft of bicycles, theft from buildings, theft from coin operated devices or machines, and all other theft not specifically classified.
Trespass	To unlawfully enter land, a dwelling or other real property.
Vandalism	The willful or malicious destruction, injury, disfigurement or defacement of any public or private property, real or personal, without consent of the owner or person having custody or control by cutting, tearing, breaking, marking, painting, drawing, covering with filth, or any other such means as may be specified by local law.
Terrorism	The willful or malicious destruction, injury, disfigurement or defacement of any public or private property [etc. as above] by domestic or foreign nationals for the purpose of making a political impact.

Note: Table descriptions provided for general information, and may not be consistent with current Oregon criminal code.

AN APPROACH TO SECURITY

FHWA guidance offers one approach to handling potential security or disaster incidents. The RTP offers six options for action.

Prevention: This has several components, ranging from the actual stopping of an attack before it occurs, to providing improved facility designs that prevent large scale destruction. Surveillance, monitoring, and sensing technologies will likely play an important role in the prevention phase of an incident.

Response: A range of responses is offered.

Mitigation: Reducing the harmful impact of an attack as it occurs and immediately after. This entails identifying the most effective routing for emergency vehicles, evacuations and effective communication systems among emergency response teams and for general public information.

Monitoring: Recognizing that an incident is underway, characterizing it, and monitoring developments. Clearly, surveillance, monitoring, and sensing technologies would be critical to this phase of incident response, as would public information.

Recovery: Facilitating rapid reconstruction of services after an incident. Depending on the degree of damage to the community and/or transportation system, regaining some level of normalcy will require bringing the transportation system back to adequate levels of operation.

Investigation: Determining what happened in an attack, how it happened, and who was responsible. This is primarily a security/police activity that reconstructs the incident and determines causality and responsibility.

Institutional Learning: Conducting a self-assessment of organizational actions before, during, and after an incident. This element provides a feedback to the prevention element in that by understanding what went wrong or right in response to an incident, steps can be taken to prevent possible new threats.

RVMPO AREA SECURITY PLANNING

Within the planning area, some specific strategies have been developed. They are discussed below in the context of national security planning initiatives.

Intelligent Transportation System (ITS) Program – Since the early 2000's a new federal transportation program focusing on information technology to address problems was developed. This Intelligent Transportation Systems program can make a major contribution toward transportation security. It can assist in all four phases of security: planning, preparedness, response and recovery. However, planners must consider that because of ITS installations' dependence on computers and electrical power, they are also more vulnerable to security threats than are many other transportation elements.

Freight – Special security planning efforts focus on freight movements. The Federal Motor Carrier Safety Administration reviews security measures with motor carriers and shippers that may be the target of terrorist attack. Its mission is to increase the

level of awareness of hazardous materials carriers to terrorist threats. The FMCSA field staff provide information in the form of recommendations and suggestions.

Transit – By law, 1 percent of 5307 urbanized funds / formula funds for transit are to be used for safety and security. The focus has been on intercity bus systems by assessing critical security needs and vulnerabilities; and training transportation personnel to recognize and respond to criminal attacks and terrorist threats, as well as in evacuation procedures. RVTD fulfills the obligation of investing 1% in safety and security by contracting with a 3rd party security firm to patrol Front Street Station, RVTD's main transportation hub in downtown Medford.

Because the security threat to bus operations is not limited to intercity services, all public transportation companies are required to have security plans. RVTD maintains a security plan for its facilities and activities. In addition, RVTD is the primary mass transportation and evacuation resource identified in the Jackson County Emergency Operations Plan.

Emergency Planning - Another aspect of providing for secure transportation has to do with the subject of "emergency planning." While transportation security is directly related to preventing attacks that are intended to harm people and damage facilities, harm modes of travel, and harm important transportation infrastructure, emergency planning is intended to respond to unforeseen natural events and disasters. A security incident is one that directly pertains to acts of terror resulting in regional, local, or specific location attacks on people, sites, facilities, or transportation infrastructure; whereas emergency response planning efforts address preparedness and response and recovery to natural disasters such as earthquakes, floods, hurricanes, violent weather, fires, and similar incidents. There are several agencies that coordinate on security and safety matters for the purpose of homeland security. The term "homeland security" refers to domestic governmental actions designed to prevent, detect, respond to, and recover from acts of terrorism, and also respond to natural disasters. Homeland security represents a concerted, national effort to protect the homeland by all levels of government at the Federal, State, and local levels, for the sole purpose of protecting the U.S. from internal and external hazards.

RVMPO PLANNING

Security planning efforts in the planning area are directed and managed by the emergency responders – police, fire, medical – representing all of the RVMPO jurisdictions. All of the agencies have collaborating on producing and maintaining emergency response plans. In areas involving transportation, public works staffs collaborate and assist the responders in both planning and incident response. Emergency coordinating organizations in the region have a long history of collaboration and cooperation. They have taken the lead in developing appropriate strategies and implementing plans. Also, they routinely coordinate drills and exercises among transportation providers to practice emergency planning.

The RVMPO's role has been through the staff who participates in both the RVMPO TAC and in emergency response planning efforts. The RTP identifies projects that assist responder efforts, most specifically in the area of ITS. RVMPO developed and

maintains the region's ITS plan in consultation with emergency responder representatives. As such, the RVMPO provides a forum for agencies and the public to examine issues and identify needs and solutions. To accomplish this, the RVMPO organized and maintains the Rogue Valley Intelligent Transportation System group (RVITS), and facilitates RVITS meetings to continue ITS planning and implementation. In 2017 the RVMPO will adopt the updated ITS plan which will help keep the Valley current with emerging technology.

Future contributions of the RVMPO are likely to focus in two areas: prevention and mitigation. Prevention planning can include: funding new strategies/technologies/projects that can help prevent events; providing a forum for security/safety agencies to coordinate surveillance and prevention strategies; finding funds for security-enhancing systems; continuing to coordinate with security officials in development of prevention strategies.

Other activities for the RVMPO could include:

- Using published sources, create annual tables of transportation security incident data by mode.

- Analyze the available databases for policy and program directions and review conclusions with appropriate lead agencies.

- Working with regional lead agencies, assist in conducting security assessments/audits for each of the transportation modes in the region, addressing physical facilities and equipment, training levels, table top exercises and response/recovery plans. The role of the RVMPO in these audits should be to provide a source of information on national developments and guidelines, and to encourage a degree of consistency among modes in terms of the quantity and quality of data collected.

- Regularly review with the Technical Advisory Committee the TIP scoring matrix and other specific funding program scoring matrices to ensure that security projects receive appropriate weighting and priority in the TIP.

- Regularly review the Tier 1 and Tier 2 project development process for the RTP to ensure that security receives adequate priority in the development of the long range project list.

VULNERABLE FACILITIES

Within the RVMPO planning area, one vulnerable facility identified by the Medford City Council is the Interstate 5 Viaduct through central Medford.

Failure of this elevated section of the interstate would cause serious disruption of north-south travel. RVMPO is considering a region-

Medford I-5 Viaduct

wide process of identifying alternate routes to I-5 and other key roadways in event of emergencies. Meanwhile Medford is looking for resources to address potential viaduct failure.

ODOT has prepared the *Oregon Highways Seismic PLUS Report* (2014) which outlined a statewide program to address seismic vulnerability and mitigate structural deficiencies. The report identified long-term (over multiple decades) mitigation strategies on state highways, including those servicing the Rogue Valley. However, a shorter-term plan is needed to ensure reasonable access to and from the Rogue Valley following a major quake.

The *Rogue Valley Seismic Event Highway Triage Approach* (2016) which is the shorter-term plan for the area. This report describes a short-term "*triage approach*" for providing reasonable access to and from the Rogue Valley on two important lifeline routes following a major quake: (1) Interstate 5 (north to Highway 58 and south to the California border) and (2) OR 140 (US 97 to I-5; and OR 140 to I-5 on OR 62). They used data from the *Seismic PLUS Report* as the basis for determining damage and repair costs. ODOT staff from Region 3 and Technical Services (Geology and Bridge Units) identified bridges and unstable slopes on Interstate 5 and OR) that would be impacted by a major Cascadia event. Then they assigned each to one of three triage categories.

Table 5.9.2: Triage Categories

Triage Categories	Total Assigned	
	Bridges	Slopes
Triage #1: Extensively damaged bridges and slopes with feasible detour routes on state or local highways that <u>would not require</u> any mitigation before a major earthquake event	22	0
Triage #2: Extensively damaged bridges and slopes without feasible detour routes on state or local highways that <u>would require</u> rehabilitation or retrofit work before a major earthquake event	17	7
Triage #3: Bridges and slopes that would sustain relatively minor damage that could be repaired under traffic within ten months (much quicker in many instances) following a major earthquake, thus <u>not requiring</u> advance mitigation work to provide reasonable access	63	131
Totals	**102**	**138**