Virginia's Long-Range Multimodal Transportation Plan 2007-2035

SECURITY

Prepared for:
Office of Intermodal Planning and Investment
October 2009

Prepared by:
Virginia Port Authority

ABBREVIATIONS AND ACRONYMS

ASTLRP	Amtrak Security Threat Level Response Plan
CBP	Customs and Border Protection
CCTV	Closed Circuit Television
CSI	Container Security Initiative
COVEOP	Commonwealth of Virginia Emergency Operations Plan
C-TPAT	Container-Trade Partnership Against Terrorism
DAS	Department of Homeland Security
DOAV	Virginia Department of Aviation
EDL	Enhanced Driver's License
ESF	Emergency Support Function
FRA	Federal Railroad Administration
FRAC	First Responder Authentication Credential
GA	General Aviation
HSAS	Department of Homeland Security's Advisory System
ICS	Incident Command System
MACS	Multi-agency Coordination System
MARSEC	United States Coast Guard's Maritime Security Levels
MOU	Memorandums of Understanding
MTSA	Maritime Transportation Security Act
NIMS	National Incident Management Systems
NRP	National Response Plan
OCP	Office of Commonwealth
SSM	Security Sensitive Materials
STATE COORDINATOR	State Coordinator of Emergency Management
TIH	Toxic Inhalation Hazards
TJTTF	Tidewater Joint Terrorism Task Force
TSA	Transportations Security Administration
TWIC	Transportation Security Administration's Transportation Worker Identification Credential
VABC	Virginia Department of Alcohol Beverage Control
VASAC	Virginia Aviation Security Advisory Committee
VDEM	Virginia Department of Emergency Management
VDOT	Virginia Department of Transportation
VEOC	Virginia Emergency Operations Center
VERT	Virginia Emergency Response Team
VFC	Virginia Fusion Center
VPA	Virginia Port Authority
VSP	Virginia State Police

TABLE OF CONTENTS

INTRODUCTION

Safety and Security are the primary concern for travelers that utilize the varying transportation mechanisms throughout the Commonwealth of Virginia. Highways, railroads, airports, and seaports link to provide efficient travel and delivery of goods. Whether travel is by air, sea, or land, the potential exists that incidents occurring within the Commonwealth's transportation infrastructure can have disastrous consequences and can restrict travel and international commerce.

TRADEOFFS BETWEEN SECURITY AND EFFICIENCY

Finding a balance between security and efficiency are major concerns for the Commonwealth of Virginia. The trade-off debate has increased exponentially in the wake of the September 11th attacks on the Pentagon and the World Trade Center Towers. Securing people and cargo includes both physical screening, regulations for transporting certain materials, and physical security of transportation infrastructure. Providing security requires time, money, and manpower. The increase in security measures directly impact the efficient flow of travel and commerce. Efficiency in this sense is the ability to move people and cargo in the shortest amount of time with the least amount of monetary investment.

Real ID

After the 9/11 Commission Report, a need was identified for a national identification standard that could be implemented at the state level. The Commission stated "at many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are". To assist the federal government in implementing such security strategies, and to comply with the Real ID Act, Virginia will incorporate new security measures. The goal of the Real ID Act is to strengthen national security by standardizing individual states' driver's license procedures. The Commonwealth of Virginia will utilize the Real ID system to ensure positive identification of individuals. The requirements and security features will increase the difficulty for terrorists that seek fraudulent state-issued licenses, improve the reliability and accuracy of drivers licenses that state governments issue, and make it easier for law enforcement agencies to detect falsified drivers licenses.

Strategies

The Commonwealth should fully implement the REAL ID compliant standard card format with enhanced security features to prevent the use of fraudulent documents. The added security features will augment the Commonwealth's and the Nation's ability to deter terrorists that attempt to use fraudulent government documents. Additionally, the Commonwealth should ensure this will comply with the federal Enhanced Driver's License (EDL) requirements. The EDL is specifically designed for cross-border travel into the U.S. by land or sea.

Transportation Worker Identification Credential (TWIC)

Similar to the Real ID system, in January 2009 the Commonwealth of Virginia implemented the Transportation Security Administration's Transportation Worker Identification Credential Program commonly known as TWIC *Phase I*. The Transportation Worker Identification Credential (TWIC) is an identification credential for personnel allowing unescorted access to Maritime Transportation Security Act (MTSA) regulated facilities. The TWIC process will screen applicants for disqualifying felonies such as espionage, sedition, treason, or a federal crime involving terrorism. The TWIC permits positive identification of the holder by law enforcement and security personnel through his or her photo, biometric information coded within the card, and enhanced security features to prevent tampering and or forgery.

Federal regulations currently being proposed will delineate the use of electronic readers designed to work with the TWIC as an access control measure (TWIC *Phase II*). The rule will address potential requirements associated with TWIC readers, such as recordkeeping requirements for owners or operators, and amendments to security plans previously approved by the US Coast Guard to incorporate TWIC requirements. The rulemaking action, once final, would enhance the security of ports and vessels by ensuring only persons who hold valid TWICs are granted unescorted access to secure areas on port facilities and vessels. It would also complete the implementation of the Maritime Transportation Security Act of 2002 transportation security card requirement, as well as the requirements of the Security and Accountability for Every Port Act of 2006, for regulations on electronic readers for use with Transportation Worker Identification Credentials.

Strategies

The Commonwealth should [disagree, this is a federal requirement, the state "will" not "should" implement Phase II of the Transportation Worker Identification Credential (TWIC) requirements for the use of biometric scanning and PIN numbers for all personnel that require unescorted access to Maritime Transportation Security Act (MTSA) regulated facilities. In addition, the Commonwealth should actively screen the Transportations Security Administration (TSA) terrorist watch list against those individuals that require unescorted access to the MTSA regulated facilities.

EMERGENCY AND DISASTER PREPAREDNESS

National Incident Management System (NIMS) / Incident Command System (ICS)

The National Incident Management System (NIMS) standardizes command management, planning and training, and the allocation of resources, communications, technologies, as well as maintenance. Such operations not only maintain the level of preparedness but also gauge how the country's resources can best be utilized. NIMS is prepared to handle any kind of incident by using two different types of management structures: the Incident

Command System (ICS) and the Multi-agency Coordination System (MACS). ICS integrates "facilities, equipment, personnel, procedures and communications" in one common organizational structure by using five major management functions: command, operations, planning, logistics and finance/administration. Such a system is able to conform easily to the "type, size, scope, and complexity" of any incident (NIMS). ICS is used as the foundation for control of an incident, not just mainly for one agency or group; MACS expands the ICS concept to ensure multi-agency groups are appropriately managed. This system can be used to combine "facilities, equipment, personnel, and communications into a common framework for coordinating and supporting incident management." This framework has been incorporated in the Commonwealth's Emergency Operations Planning.

Strategies

The National Incident Management System and Incident Command Systems should be continually and aggressively exercised to strengthen the capabilities of the Commonwealth to ensure standardized command management, coordinated planning and training initiatives, and adequate communications in the event of catastrophic emergencies.

Commonwealth of Virginia Emergency Operations Plan (COVEOP)

The Commonwealth of Virginia Emergency Operations Plan (COVEOP) is Virginia's all-hazard emergency response and recovery plan. The plan recognizes that emergency response begins at the lowest jurisdictional levels and is designed to rapidly provide resources and coordinate responses. Aligned with the National Response Framework, the COVEOP is built upon scalable, flexible, and adaptable coordination to support multijurisdictional response. Initiated upon the Governor's declaration of a state of emergency, the COVEOP assigns specific duties and responsibilities to agencies for carrying out specific emergency response actions. The COVEOP enhances coordination of state support to local government, businesses, and citizens. The Virginia Emergency Operations Center (VEOC) provides centralized direction and control for the Governor or his designee to coordinate guidance and assistance to local governments and state agencies. The State Coordinator of Emergency Management (State Coordinator) directs the activities of the Virginia Emergency Response Team (VERT) in support of localities from the VEOC.

Strategies

The Virginia Emergency Operations Center should continue to exercise the COVEOP with state agencies, local governments, for-profit and no-profit groups, and citizens to strengthen the Commonwealth's all-hazards emergency coordination efforts.

Evacuation Routes

The Atlantic hurricane season creates uncertain weather conditions throughout the Commonwealth. The Virginia Department of Emergency Management (VDEM), Virginia Department of Transportation (VDOT), Virginia State Police and the Virginia National Guard have partnered to conduct annual emergency preparedness exercises. The exercises are designed to test the Commonwealth's ability to reverse the interstate highway system for evacuations. The reversal changes the direction of all eastbound lanes and diverts westbound traffic to both sides of the interstate.

Strategies

VDEM, VDOT, VSP, and the Virginia National Guard should continue the practice of conducting annual exercises that include the lane reversals of the Commonwealth's highway system. The lessons learned from each event should be closely analyzed, the problems indentified, and solutions implemented to ensure safe and effective emergency evacuation of citizens.

First Responder Authentication Credential (FRAC)

The Commonwealth is currently in the process of implementing the First Responder Authentication Credential (FRAC) program. The FRAC Program will allow emergency managers to verify the identity and other pertinent information of Emergency Responders at incident scenes, as well as, identify the first responder's status within Sectors, Agency, or Emergency Support Function (ESF) which supports the National Response Plan (NRP). In addition, the FRAC identification card confirms qualifications of first responders to enable incident commanders to rapidly deploy personnel. The Commonwealth has initiated the first roll-out of the FRAC. The FRAC program is a multiyear implementation strategy for the Northern Virginia, District of Columbia and the Hampton Roads regions.

Strategies

The Office of Commonwelath preparedness (OCP) is standardizing the criteria for establishing the need of a First Responder Identification Credential (FRAC). The criteria would eliminate contention among the various state, local, and for- and non-profit groups that have a vested interest in the program.

PORT/CARGO SECURITY

The United States Coast Guard's Maritime Security Levels (MARSEC), which parallel the Department of Homeland Security's Advisory System (HSAS), will continue to play a significant role for the Commonwealth and the Port of Virginia in 2040. MARSEC is "set to reflect the prevailing threat environment to the marine elements of the national transportation system," which in turn causes an increase in security measures (Coast

Guard website). Such tasks preformed by Customs and Border Protection (CBP), Port Police, and other security agencies are a viable part of modern maritime commerce. Security measures will increase, thus making inspections of containers, personally owned vehicles, and commercial traffic more stringent. These inspections, however productive to security, increase congestion at port gates and portals, container yards, and port berths.

Strategies

The Commonwealth of Virginia should continue to strengthen and secure the infrastructure of the maritime seaports. The port will continue to improve the strength of security layers through enhanced electronic surveillance and information assimilation.

Container Security Initiative (CSI)

Containerized cargo shipping is the primary method for international trade. Economic infrastructures have increasingly become the target of terrorist organizations. The rationale of the Container Security Initiative (CSI) is the use of reciprocity agreements with host nations to screen cargo prior to import into the United States. Prescreening is conducted using automated information systems to target suspect shipments. Detection technology such as gamma radiation detectors and imaging equipment are utilized to prescreen the targeted containers.

Container- Trade Partnership Against Terrorism (C-TPAT)

The Container-Trade Partnership Against Terrorism (C-TPAT) is a voluntary federal initiative to increase cargo and border security. United States Customs and Border Protection encourage participation from owners within the supply chain. C-TPAT provides greater supply chain security by working with international supply chain members to ensure the integrity of security practices. The supply chain covers importers, carriers, consolidators, customs brokers, and manufacturers to align approved security measures with current business practices.

Federal Bureau of Investigations: Tidewater Joint Terrorism Task Force (TJTTF)

The Federal Bureau of Investigation has the primary responsibility of investigating terrorism in the United States and has chosen to partner with other agencies in these efforts. In Hampton Roads, the Tidewater Joint Terrorism Task Force is composed of local, state and federal agencies to investigate terrorism within the region. The Commonwealth of Virginia has allocated resources from the Virginia State Police (VSP), Virginia Port Authority (VPA), and Virginia Department of Alcohol Beverage Control (VABC) to ensure that the shared goals of protecting the Commonwealth and the country as a whole are met.

Command and Control

Establishing solid command and control capabilities at the onset of any incident is the premise of both the National Incident Management System (NIMS) and the Incident Command System (ICS). The Virginia Port Authority has fully integrated existing Closed Circuit Television (CCTV) systems, emergency response communications and dispatching, and actionable procedures into one platform. The integration enhances the Port's ability to maintain communications throughout the three facilities; Norfolk International Terminals, Portsmouth Marine Terminal, and Newport News Marine Terminal. The new system supports continuity of operations and emergency response, credentialing, enhances real-time information exchange within the maritime domain awareness, improves risk management, and is in full compliance with the Customs-Trade Partnership Against Terrorism (C-TPAT). The integration of legacy technologies with current and future technologies creates an emergency response solution that integrates security functions into a central command and control system, effectively allowing the agency to mitigate incidents and ensure continuity of operations through the use of the Emergency Operations Plan. The fusion of data will be the foundation for sharing with federal, state, and local authorities. The Virginia Fusion Center (VFC) provides analytical assistance in support of investigations and operations. The Virginia Emergency Operations Center provides a centralized direction and control operation to coordinate the provision of guidance and assistance in accordance with the COVEOP.

HIGHWAY INCIDENTS

The Virginia Department of Transportation (VDOT) has revamped the emergency response plan to improve communicating to the public, response times to incidents, standardization of incident response through the implementation of the Incident Command System (ICS) and the National Response Plan (NRP), and intrastate agency coordination. The new plan will allow the Commonwealth and VDOT to mitigate both minor and major incidents to include weather, hazardous material spills, and acts of terrorism.Actions will be regionally specific but all will include anti-icing, several measures to improve traffic flow, as well as primary and continuing education for agency employees and the public. The plan implemented by VDOT will significantly contribute to the overall security and safety throughout the Commonwealths' transportation infrastructure.

INFORMATION TECHNOLOGY

Information security poses significant challenges for not only the Commonwealth of Virginia, but other states throughout the country. The Commonwealth of Virginia has taken steps to build upon the already robust information technology infrastructure. The Commonwealth has invested significantly to maximize the use of technology to facilitate, improve, and maintain high standards in the delivery of services.

Strategies

The Commonwealth has established five strategic objectives. First, the Commonwealth will build information technology infrastructures to support e-government services for public access to information and services via the internet. Second, the Commonwealth will develop partnerships to bridge existing organizational boundaries to promote technical resource sharing. Third, a technologically sound environment will be created to ensure reliability, security, and integrity. Fourth, to develop a reputation for high technology performance to enable the Commonwealth to utilize technology in an open, transparent, and accountable government. Last, the Commonwealth will increase productivity through the use of new technology. Agencies of the Commonwealth will apply proven technologies to enhance productivity and workforce retention.

AIRPORT SECURITY

The Transportation Security Administration (TSA)is responsible for the security of commercial service airports nationwide. The Virginia Department of Aviation (DOAV) is committed to overseeing the security of Virginia's General Aviation (GA) airports while allowing for seamless transportation within the Commonwealth. Virginia's GA security posture is based on the Homeland Security Advisory System (HSAS). The Department of Aviation has teamed with the Virginia State Police (VSP) to conduct security assessments ofthe 57 public-use GA airports on a three year schedule. Currently, security improvements including; security plans, signage, lighting, surveillance systems, and fencing, are funded by DOAV on a first-come, first-served basis. If questions arise about project feasibility, DOAV works with its VSP, TSA, and DHS partners for their input and recommendations. However, a prioritization system based on deficiencies noted in the VSP assessments has been developed. Quarterly security meetings are held by members of the Virginia Aviation Security Advisory Committee (VASAC). This committee consists of state and local law enforcement, federal security agencies, and industry partners. Its purpose is to develop security "best practices" and discuss ongoing GA security initiatives.

RAILROAD AND TRANSIT SECURITY

High profile terrorist attacks on rail systems in Madrid, London, and Mumbai provide troubling illustration to persistent warnings that the U.S. public transportation system is a vulnerable target for terrorists. But passenger rail is not the only, and perhaps not even the gravest concern. Much of the 160,000 miles of railroad track in the United States transports freight, including highly toxic chemicals. These shipments often have minimal security, even though they pass through populated areas, endangering thousands of lives. Since 9-11, security enhancements have included:

- Closing gaps in fencing surrounding the rail station in order to better secure the rail facility.

- Improving the facility's lighting in order to improve surveillance and decrease the site's attractiveness to terrorists.
- Installing blast resistant trash receptacles to absorb a blast if a bomb is placed while still providing passengers with receptacles for their trash.
- Installing close-circuit television to increase security personnel's visibility over the rail facility.
- Posting signs to educate riders about potentially dangerous unattended packages and evacuation procedures in the event of an emergency.
- Emphasizing to personnel and passengers that they have a role in security by reporting unattended packages and luggage, and suspicious behavior.

Rail Security is commonly separated into two parts: passenger rail and freight rail. Each type has its own security concerns. Passenger rail is vulnerable because the systems are most often located in densely populated cities with numerous stops, allowing for easy movement and escape. In addition, the nature of mass transportation relies on accessibility and quick service, both of which would be harmed by airport-like security measures. Freight rail, although often not traveling through dense urban areas, transports approximately half of the US's hazardous waste materials. As prior accidents have shown, these materials can cause great damage. The nature of freight rail would also prevent airport-like security to be imposed. As a commercial entity, freight rail must compete with trucks and air in order to effectively serve as transporters of goods.

Passenger Rail

Each year Americans make more than 3.5 billion trips on intercity trains, commuter rails, and subways. The abundance of passengers, combined with the need for easy access, makes securing passenger railways a daunting task. Absolute security can never be achieved, and experts caution against extreme security measures, which they say would disrupt how transportation systems function while offering no guarantee against attack. The Security located at rail stations centers primarily around law enforcement of the station. The officers at Amtrak, for example, do not focus their training on counter terrorism, but do perform security evaluations of their respective stations. Amtrak also created a Security Coordinator Program. Within each Amtrak division, a Security Coordinator works closely with Amtrak Police and Security personnel to review the security components and steps of the Security Threat Level Response Plan (ASTLRP) and to ensure that employees within their division are undertaking the required steps.

In an attempt to balance security and accessibility, rail companies have taken measured precautions to help prevent attacks. These include random searches of passengers and baggage, increased presence of security officers and bomb-sniffing dogs, increased video surveillance, removal or hardening of trash cans so they cannot hide bombs, and encouraging passengers to report suspicious activity. Additionally, many have sought to bolster their ability to react to emergencies in order to minimize the impact of an attack. This includes emergency planning, hiring and training emergency personnel, and purchasing emergency equipment such as radios. By mitigating the potential impact of a

terrorist attack, experts say, rail companies could discourage some terrorists from targeting them.

On 20 May 2004 the Department of Homeland Security (DHS) issued Security Directives (SD) requiring protective measures to be implemented by passenger rail operators. The measures instruct commuter, transit and inter-city passenger rail systems to comply with requirements that range from removing or replacing station trash cans to utilizing canine explosives detection teams. The directives, which are administered by the Transportation Security Administration (TSA), took effect on 23 May 2004. The directives apply to all passenger rail owners/operators. These include light rail systems and inter-city passenger rail systems such as Amtrak. The mandatory measures cover a broad range of security issues and provide flexibility to meet the specific needs of rail operators. They substantiate existing best practices in the rail industry and will ensure enhanced security across the nation's passenger rail systems. The directives require rail operators to take a number of steps, among them:

- Rail owners/operators must designate coordinators to enhance security-related communications with the TSA.
- Passengers and employees will be asked to report unattended property or suspicious behavior.
- At certain locations, operators will be required to remove trash receptacles, except clear plastic or bomb-resistant trash containers.
- When needed, canine explosive teams may be utilized to screen passenger baggage, terminals and trains.
- Facility inspections will be conducted by rail operators for suspicious or unattended items.
- Rail operators will ensure that security is at appropriate levels consistent with the DHS established threat level.
- Conducting comprehensive vulnerability assessments of rail and transit networks that operate in high-density urban areas.
- Training for rail personnel in preventing and responding to potential terrorist events.
- Developing new technologies including chemical and biological countermeasures.

Strategies

Through the Office of Commonwealth Preparedness, complete an assessment of passenger security measures implemented to-date and areas for enhancements and improvements. In particular, review and modify as necessary Memorandums of Understanding (MOU) with federal, state, local and private law enforcement and first responders to ensure railroad security goals and objectives are being met. Develop MOUs where gaps exist.

The City of Norfolk, working with local, state and federal partners will employ the latest in security measures during the construction of the light rail "The Tide."

Freight Rail

Many of the tracks that carry passenger trains run parallel to those carrying freight shipments throughout the United States, meaning rail cargoes often travel along the same heavily populated corridors. Much of the freight presents little danger to people living near the tracks, but some does—particularly certain industrial chemicals. Should one of these tanks rupture—either from a terrorist attack or an accident—the results could be catastrophic. The Federal Railroad Administration (FRA) has 415 inspectors who ensure that rail freight conforms to federal regulations for transporting hazardous materials. Those regulations require rail carriers to implement security plans, including special training for their employees. The DHS and VDOT offer a list of voluntary security practices for hazmat carriers, including criminal background checks for employees, regular training drills, and designating a liaison to government emergency response agencies.

Strategies

Continue to improve partnerships with the Class I railroads, through membership within the Virginia Fusion Center and Commonwealth Preparedness Group. The Office of Commonwealth Preparedness and Virginia Department of Emergency Management will coordinate with all railroads to ensure the DHS grant program aligns with Commonwealth goals. Direct liaison with railroads will maximize DHS grant funding opportunities. Specifically focus on funding security initiatives for freight rail carriers that transport Rail Security-Sensitive Materials (SSM) through designated high population density areas and freight railroad car owners that transport materials that are poisonous by inhalation/toxic inhalation hazardous (TIH). Rail SSM includes certain explosives, materials poisonous by inhalation, and Class 7 radioactive materials; and Rail TIH includes anhydrous ammonia but excludes residue quantities of these materials.

The Office of the Commonwealth Preparedness will develop protocols to review railroad vulnerability assessments and security plans operating within the state.