APTA STANDARDS DEVELOPMENT PROGRAM

STANDARD

American Public Transportation Association
1300 I Street, NW, Suite 1200 East, Washington, DC 20006

APTA SS-SIS-S-017-21

Published: March 23,2021

Infrastructure & System Security Working Group

Security Risk Assessment Methodology for Public Transit

Abstract: This standard proposes a methodology for determining security risk in public transportation systems.

Keywords: assessment, consequence, mitigation, risk, risk tolerance, security, severity, threat, transit security, vulnerability

Summary: This document provides a methodology to assess security risk for public transportation systems. It defines the elements of a Security Risk Assessment to include threat, vulnerability, likelihood and consequence. Using this methodology to assess security risk provides transit agencies a sound process to determine risk and develop mitigation measures or controls to improve their risk profile.

Scope and purpose: The purpose of this document is to provide public transit and rail agencies with guidance for defining and assessing security risk in a public transportation environment. The methodology can be adapted to other industries with modification to the criteria.

Table of Contents

List of Figures and Tables

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Transit Infrastructure Security Working Group**, which provided the primary effort in the drafting of this document.

At the time this standard was completed, the working group included the following members:

Lurae Stuart, *Chair*
Mark Uccardi, *Vice Chair*

Galen Bennett, *Sound Transit*
Michael Birch, *RAPT Dev USA*
Don Burr, *Community Transit*
Ryan Chelski, *Sound Transit*
Neil Crosier, *King County Metro*
Dean Fajerski, *TSA*
Kevin Franklin, *BART*
Paul Huston, *VIA Rail Canada*
Andy Niero, *TSA*
Mark Norton, *King County Metro*
Stephan Parker, *Transportation Research Board*
Rob Pascoe, *King County Metro*
Jacob Peltier, *Community Transit*
John Plante, *METRA*
Branden Porter, *Sound Transit*
Jason Powell, *Metro St. Louis*
Charles Rappleyea, *WSP USA*
Sean Ryan, *MTA Metro-North Railroad*
Harry Saporta, *WSP USA*
Lurae Stuart, *WSP USA*
Brian Taylor, *retired*
Kirsten Tilleman, *WSP USA*
Peter Totten, *AECOM*

Project team

Polly Hanson, *American Public Transportation Association*
Eric Halzel, *Eagle Hill Consulting*

Introduction

This introduction is not part of APTA SS-SIS-S-017-21, "Security Risk Assessment Methodology for Public Transit."

A key objective of any public transportation system is to provide safe, secure and reliable public transportation services. Transit agency personnel, consultants and contractors are expected to implement appropriate security considerations throughout the planning, design, construction, fabrication, installation, testing, preoperational and operational system phases of transit during the life cycle of the system.

This standard is intended to complement other documents or reports that address security for public transportation. It builds on and incorporates information described in the series of the APTA Security Standards Program documents. They should be reviewed and applied where applicable. Find APTA's Security Standards Program documents at www.apta.com.

Security Risk Assessment Methodology for Public Transit

1. Overview

A Security Risk Assessment, also known as a Threat and Vulnerability Assessment (TVA), is intended to evaluate a transit/rail system's susceptibility to security threats and to identify vulnerabilities and potential consequences. The assessment forms the basis for design measures, plans and procedures to be implemented to reduce or mitigate the security risk.

The process for determining security risk begins with the identification and grouping of agency assets critical to operations; the assets' attractiveness as targets for crime, a security incident or a terrorist attack; their vulnerability to the impacts of a successful criminal or terror incident; and the consequences of a successful incident. Critical assets are defined as those assets required to provide services for the system. Specifically, critical assets are defined as the following:

- **People:** Passengers, employees, visitors, vendors, surrounding businesses and communities, and contractors working within the transit environment.
- **Property:** Including but not limited to stations and stops, maintenance facilities and yards, administration facilities, control or dispatch centers, rolling stock, tracks, tunnel portals, bridges, crossing protection devices, parking facilities, wayside facilities (signaling equipment, communication rooms/cabinets and signal rooms/cabinets), fare vending machines, equipment technology, and communication/industrial control systems.
- **Information:** Operations and maintenance procedures, security procedures and assessments, computer network information, and passwords and facility access codes.

1.1 Stakeholder considerations

Security for transit systems should be based on the assessed risk to the system to ensure that resources are allocated judiciously and provide the optimal benefits to the system's security. Consideration should be given to the needs and requirements of agency stakeholders, such as police and security.

1.2 Benefits

Transit and rail agencies that apply this standard to their transit operation will:

- understand how to identify and assess threats to their transit system and system elements;
- recognize vulnerabilities to their system that increase the likelihood of a security event;
- measure the value of the likelihood of an event against the severity or consequence to define security risk;
- provide a basis to allocate resources appropriately within the agency; and
- have a reliable, repeatable methodology on which to base security recommendations and allocate resources.

2. Security Risk Assessment

Transit agencies should complete a system-wide Security Risk Assessment to determine the exposure of the system's people, assets, operations and infrastructure. A risk-based approach that factors threat, vulnerability and consequence should be used for this purpose. The methodology described in this standard provides one such approach for public transportation systems.

2.1 Systemwide and site-specific Security Risk Assessments

Transit agencies shall complete system-wide Security Risk Assessments to determine the threats, vulnerabilities and consequences to their overall systems and properties. The assessment should compare and assess all agency transit modes, assets and facilities that make up the system. Alternatively, when agencies want to determine risk to a specific site or asset, they should perform a site-specific Security Risk Assessment.

2.2 Security Risk Assessment methodologies

The methodology contained in this standard is one of many that could be employed to assess security risk, to include the Public Transit Risk Assessment Methodology (PT-RAM) jointly developed by the Federal Emergency Management Agency (FEMA) and the Transportation Security Administration (TSA). There are also other resources that provide guidance for Security Risk Assessments. Agencies should evaluate the Security Risk Assessment methodologies against their own needs to determine which methodology is most appropriate given their characteristics (e.g., sub-modes, ridership, location).

> **NOTE:** It is not appropriate to use the safety hazard model of probability and severity to measure security risk. This methodology does not factor in all the elements present in a security environment and will not provide the transit agency with a credible security risk determination. In particular, the safety analysis methodology does not account for an adversary that thinks and can adapt to defensive countermeasures.

For more information regarding risk assessments, consider the following resources:

- FEMA, "Threat and Hazard Identification and Risk Assessment (THIRA)" and "Stakeholder Preparedness Review (SPR) Guide," May 2018.
- National Institute of Standards and Technology, "Guide for Conducting Risk Assessment," NIST Special Publication 800-30 Revision, September 2012.
- Department of Homeland Security, "National Infrastructure Protection Plan (NIPP)," 2013.
- State Government of Victoria, Department of Transport, "Security Risk Assessment for Transit Operations," 2012.
- American Association of State Highway and Transportation Officials (AASHTO), "A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection," 2002.
- Department of Homeland Security, "Integrated Rapid Visual Screening Series (IRVS) of Mass Transit Stations," Buildings and Infrastructure Protection Series, BIPS 02, 2011.
- FEMA, "Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings," FEMA 452, 2005.

2.3 Timing and schedule

Security Risk Assessments should be evaluated periodically to confirm that they adequately address the security risks faced by the agency and provide the basis to allocate resources to reduce the risk. Agencies must update the Security Risk Assessment or TVA if any of the following occur:

- change in threat environment
- change in system operation
- change in project phases, starting at conceptual design/planning
- security incidents (after-action)

2.4 Sensitive Security Information

Sensitive Security Information (SSI) is information about security, operations, facilities, or other assets or capital projects whose disclosure would be detrimental to the security of transit employees or customers.

> **NOTE:** SSI is defined in 49 CFR §15.5 as "…information obtained or developed in the conduct of security activities, including research and development, the disclosure of which the Secretary of DOT has determined would—
>
> - Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);
> - Reveal trade secrets or privileged or confidential information obtained from any person; or
> - Be detrimental to transportation safety."

By law, transit agencies are required to categorize and protect SSI. Protecting SSI means restricting its distribution and controlling access to it. By law, SSI is not subject to disclosure under the Freedom of Information Act (FOIA)[1] or state "sunshine laws." It is also not available under discovery in civil litigation, and it is not required to be part of the record in federal rulemaking.

> **NOTE:** "Sunshine laws" are statutory laws based on the idea of openness in government, with public access to records and meetings and the conduct and activities of government.

Requirements for managing SSI are contained on the regulations in 49 CFR, Parts 15 and 1520. Security Risk Assessments that include system vulnerabilities fall under the SSI regulation. Additional information regarding SSI can be found in the regulation and in "Sensitive Security Information (SSI) Designation, Marking and Control," FTA, March 2009.

Security risk assessments are considered SSI. Each agency should designate a person who has the authority and capability to determine SSI for the agency and implement the agency's SSI policy. Agencies should be cautious and thoughtful about what they mark as SSI to ensure that materials meet SSI definitions as described in the regulation.

1. Title 5 United States Code (USC) §552

3. Security Risk Assessment process and methodology

3.1 Acceptable risk

The FTA defines acceptable risk as follows:

> "The level of risk deemed 'acceptable' is determined on the basis of the agency's safety performance criteria, industry standards, public opinion regarding such risk, and political and legal considerations. If the risk does not meet the acceptability criteria, an attempt must always be made to reduce it to a level that is acceptable using appropriate mitigation procedures."

It should be noted that when a transit agency "accepts" a risk, this does not mean the risk is eliminated; some level of risk still remains (residual risk). However, the agency has accepted that the risk is sufficiently low that it is outweighed by the benefits of the existing operation.[2]

The same concept of acceptability applies to security. Security risk, like safety risk, is rarely eliminated, and there is always some risk that must be accepted (security risk and safety risk are only ever eliminated if the situation in which the risk exists is eliminated). There is also a cost or resources factor in reducing risk. The concept of "as low as reasonably practicable" (ALARP) should be applied where necessary to assess the cost/benefit of applying additional measures of mitigation in order to achieve residual risk that is as low as reasonably practicable.

The ALARP principle considers the fact that infinite time, effort and money could be spent on the attempt at reducing a risk to zero but that doing so is usually not practical. The principle is not simply a quantitative measure of benefit against detriment; it is more accurately a best common practice of judgment of the balance of risk and societal benefit. ALARP does not represent zero risk.

For a risk to be ALARP, it must be possible to demonstrate that the cost involved in reducing the risk further would be grossly disproportionate to the benefit gained; that is, the greater the risk, the more resources that should be spent reducing it, and the greater the bias on the side of safety. The costs could marginally outweigh the benefits, yet the measure could still be reasonably practicable to introduce in order to reduce risk.

3.2 Qualitative vs. quantitative assessment

Risk assessments can be either qualitative or semi-quantitative depending on the level of risk, the amount of data available to the assessor and the methodology used. Qualitative analysis is entirely appropriate for assessment of risks that are found in standard industry practice or common experiences if appropriate expertise is utilized. There are methodologies that utilize quantitative analysis, but quantifying human intent and capability is challenging and frequently changes. There is always some level of subjectivity, even in a security risk quantitative assessment.

3.3 Security Risk Assessment process

In order to ensure that the transit agency has considered security risks, such as crime or acts of terrorism, it is crucial to apply a methodological approach and process to security risk management. Periodic and recurring assessment of risk is consistent with the requirement of the system security life cycle and ISO 31000 Risk Management standard.

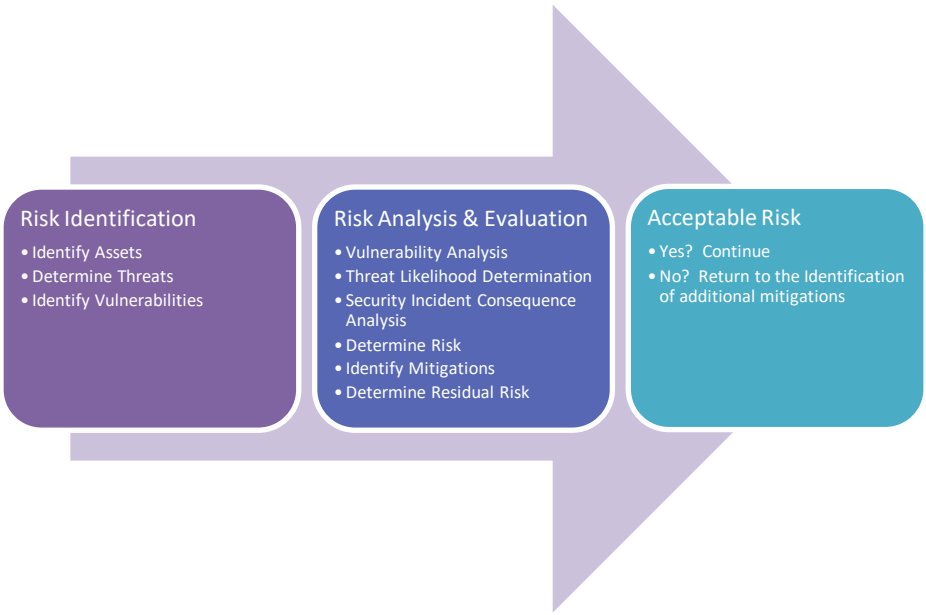
2. "Transit Safety Management and Performance Measurement," FTA, April 28, 2014

The risk assessment process should include the following:

- Identify the critical assets.
- Identify the threats.
- Identify the vulnerabilities.
- Identify the likelihood of an attack/incident.
- Identify the consequences/impacts of an attack/incident.
- Assign the initial risk index to determine the basis for risk decision criteria.
- Identify potential mitigation measures/countermeasures.
- Determine residual risk acceptability.

See **Figure 1**.

FIGURE 1
Security Risk Assessment Process



3.4 Target attractiveness

Target attractiveness varies depending upon threat actor motivations and goals, but in general the following criteria are useful in determining the potential for target selection:

- potential for public impact, damaging the society and ecosystem as a whole
- protection of target and target predictability
- potential for mass casualties
- potential for global significance or visibility to either the threat actor or the target
- target permanently or frequently available
- potential for major political or economic impact
- potential for economic gain
- ease of accessibility
- perceived “iconic” status

3.5 Asset identification

As part of the overall Security Risk Assessment process, it is important to identify the critical assets of the transit agency. Assets are anything that support the transit agency's system and operations. Often the concept of criticality is part of the identification of assets. Understanding how critical a specific asset is to the transit agency is another element of focusing resources on those assets that have the most potential to impact the system. For many transit systems, all assets are critical to how they function. For large agencies, determining criticality of the assets and focusing on those critical assets may be necessary prior to performing a security assessment.

3.5.1 People

People are integral to any system, and successful realization of an adverse security event upon people has the ability to cause mass casualty and/or operational disruption. The people who may be affected by a terrorist threat or criminal act include passengers, transit agency employees, visitors, vendors, surrounding businesses and communities, and contractors working within the public transport environment.

3.5.2 Rolling stock

Rolling stock consists of revenue and maintenance vehicles. These vehicles interface with nearly all components of the transit agency network: stations and stops, terminals, tracks, guideways, and administrative and maintenance/storage facilities.

3.5.3 Infrastructure

Infrastructure is the set of physical elements that provide the framework in which a structure or facility operates and functions. The elements enable and facilitate the execution of certain activities. Infrastructure refers to all the stationary assets in a system, such as passenger stations, real estate, buildings, bridges and tunnels, control centers/dispatch, tracks or guideways, communications, and other components necessary to support transit agency operations.

3.5.4 Information and control system

Most transit systems rely on computerized networks to facilitate operations and enhance efficient service delivery. Many safety-critical information systems also use software applications to control and operate systems. An example includes train control systems. The trend toward full computerized control over transportation infrastructure increases the potential for attacks, because increased interconnectivity and interdependence among networks creates vulnerabilities that make systems more accessible to malicious cyberattacks. The consequences of a cyberattack can be disastrous, resulting in loss of life and/or catastrophic damage.

3.5.5 Reputation

Reputation is another asset of a transit or rail agency that can be damaged or impacted by security incidents. Agencies that are not protective of their reputation by managing their risks can find themselves with additional oversight by federal or state entities or scrutiny and criticism by the public. They may also have their funding opportunities impacted by the reduction of confidence.

3.6 Threats

Security threats are defined as deliberate actions intended to cause injury or death to people and/or damage to or loss of critical assets. The threats (or attack types) to a specific transit agency may generally be the same as those faced by other similar transit agencies, but it is critical to understand the threats specific to the transit agency doing the assessment, as it can experience varying levels of threat. A threat is characterized as the combination of both intent and capability of a threat actor or threat source to realize a threat or attack against

an asset. It is possible to separately analyze the intent and the capability, but this type of analysis requires specific information and intelligence about specific threat actors and is beyond the scope of this standard.

Determination of security threats is always evolving and requires analysis to be performed as a qualitative assessment based on past performance and reliable intelligence. The nature of a threat actor's intent and capability continues to evolve and must be continually updated. Transit agencies can access historical records of manifested threat events across regional, national and international transportation modes from reliable open-source information to provide data to support security threat evaluation. Agencies can use local, state and federal sources for threat information or use a combination of sources for threat data. If the security assessment is contracted, then transit agencies should ensure that the data utilized for the threat evaluation is current and applicable to their local transit agency environment. **Table 1** provides examples of different threat categories.

TABLE 1
Threat Category Examples

Threat Category	Examples
Criminal	• Vandalism and trespassing • Organized crime • Theft • Insider threat (current/former staff)
Terrorism	• Domestic extremist groups/individuals • Transnational extremist groups • Homegrown violent extremists (HVEs) • Single-issue groups/individuals
Hostile state	• State-sponsored hostile actors
Civil unrest	• Protests

3.6.1 Crime

The majority of crime committed on public transit does not pose a physical threat to passengers but may erode passengers' confidence and sense of security, make passengers feel intimidated, and lead to more serious crime conditions, deterring passengers from using the system.

Public transportation operators face criminal threats from three primary classifications, illustrated in **Table 2**: crimes against people, crimes against property and other crimes committed on public transportation property. Other crimes committed on public transportation property generally are those that affect quality of life. Though these are usually minor, they degrade the quality of transportation service and interfere with passengers' use of the transportation system.

TABLE 2
General Crime Categories and Examples

Threat Category	Crime Types Within Category
Crimes against people	Assault, homicide, sex offenses, human trafficking
Crimes against property	Arson, cargo theft, vandalism, robbery, burglary, sabotage, vehicle theft
Quality of life/societal crime	Fare evasion, vagrancy, loud music, drinking, disorder

3.6.2 Terrorist threat

Terrorists continue to target public transit systems, as seen in the March 2016 bombing of the Brussels Metro that killed 13, discovery of an improvised explosive device in October 2016 in the London Underground, and the December 2017 attempted suicide bombing in the New York subway. Specific threats to individual transit systems should be assessed in discussion with local, state and federal law enforcement agencies. Typical examples of terrorism threat types are listed in **Table 3**.

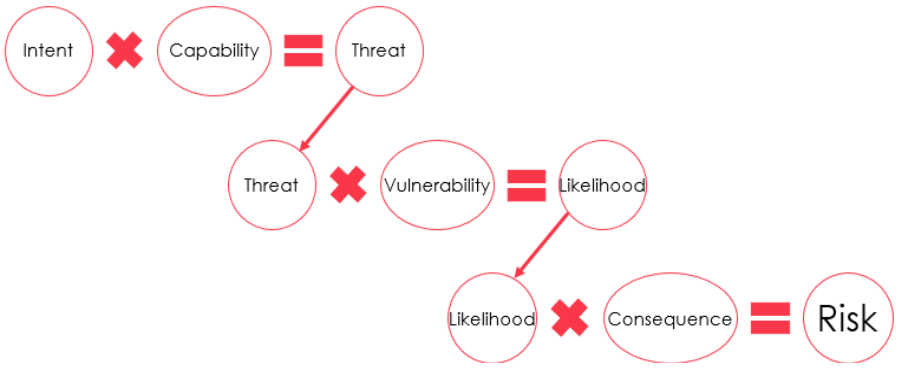
TABLE 3
Examples of Threat Types

Explosives	Improvised explosive device (IED), vehicle-borne improvised explosive device (VBIED), person-borne improvised explosive device (PBIED)
Chemical, biological, radiological	Toxic chemicals, biological agents, radiological dispersion devices
Arson	Improvised incendiary device (IID)
Active attacker	Use of small arms and other weapons of opportunity, such as edged weapons, vehicle ramming
Complex coordinated attack	Attack by a team or teams of armed individuals
Standoff attack	Weapons deployed from a distance, unmanned aircraft system (UAS)
Cyberattack	Viruses, malware, ransomware, phishing, denial-of-service attacks
Hoax call/device	Intentional false alarm or threat that potentially disrupts operation
Suicide	Death caused by self-directed injurious behavior with intent to die as a result of the behavior, suicide attempt

3.7 Security risk methodology implementation

Application of the methodology is a sequentially stepped process, as illustrated in **Figure 2**. Each step in the assessment looks at one component of security risk.

FIGURE 2
Security Risk Methodology Process



3.8 Threat rating

Threat level is based upon the combination of intent and capability to carry out the threat. Use of this comparison helps determine if a threat is realistic or credible. **Table 4** details threat ratings based on intent and capability measures. Information on intent and capability can be provided by law enforcement, fusion centers, Information Sharing and Analysis Centers (ISACs), neighborhood data, TSA/DHS, or through other security coordination activities. **Table 5** explains the threat rating definitions.

TABLE 4
Threat Rating Matrix

Intent	Capability				
	Similar exploit has been used	Operational capability confirmed by credible evidence	Some evidence that operational capability exists; not confirmed	No evidence of operational capability but feasibility confirmed	No evidence of capability and feasibility unconfirmed
Tactic has been used in the past, and a similar attack may be planned	**Very High**	**Very High**	**High**	**Medium**	**Low**
Tactic has been used before, and it is credible that it is being considered for further use	**Very High**	**High**	**High**	**Medium**	**Low**
Tactic has not been used before but is under consideration	**High**	**High**	**Medium**	**Medium**	**Low**
Tactic has not been used before, but it may be under consideration	**Medium**	**Medium**	**Medium**	**Low**	**Very Low**
Tactic has not been used before and is not known to be under consideration	**Low**	**Low**	**Low**	**Very Low**	**Very Low**

TABLE 5
Threat Rating Definitions

Threat Rating	Threat Rating Definition
Very High	Significant and proven threat present based upon demonstrated intent and demonstrated capability.
High	Threat present based upon stated/demonstrated intent with demonstrated capability.
Medium	Medium-level threat exists based upon either strong intent or some degree of stated/demonstrated capability.
Low	General threat exists and should be monitored; no proven intent or demonstrated capability.
Very Low	General threat may exist with intent and capability/feasibility unconfirmed.

Table 6 demonstrates how to apply the intent and capability by assessing three types of threats facing public transportation. Threat credibility is not fixed but can evolve over time and should be assessed regularly to understand how threats might impact the transit environment.

TABLE 6
Example Threat Ratings

ACTIVE ATTACKER					
Capability	No evidence and feasibility unconfirmed	No evidence of operational capability, but feasibility confirmed	Some evidence that operational capability exists; not confirmed	Operational capability confirmed by credible evidence	Similar exploit has been used
Intent	Tactic has not been used before and is not known to be under consideration	Tactic has not been used before, but it may be under consideration	Tactic has not been used before but is under consideration	Tactic has been used before, and it is credible that it is being considered for further use	Tactic has been used in the past, and a similar attack is planned
Threat Potential	Very Low	Low	Medium	High	Very High
HIJACKING OF TRANSIT VEHICLE					
Capability	No evidence and feasibility unconfirmed	No evidence of operational capability, but feasibility confirmed	Some evidence that operational capability exists; not confirmed	Operational capability confirmed by credible evidence	Similar exploit has been used
Intent	Tactic has not been used before and is not known to be under consideration	Tactic has not been used before, but it may be under consideration	Tactic has not been used before but is under consideration	Tactic has been used before, and it is credible that it is being considered for further use	Tactic has been used in the past, and a similar attack is planned
Threat Potential	Very Low	Low	Medium	High	Very High
CYBERATTACK, DENIAL OF SERVICE					
Capability	No evidence and feasibility unconfirmed	No evidence of operational capability, but feasibility confirmed	Some evidence that operational capability exists; not confirmed	Operational capability confirmed by credible evidence	Similar exploit has been used
Intent	Tactic has not been used before and is not known to be under consideration	Tactic has not been used before, but it may be under consideration	Tactic has not been used before but is under consideration	Tactic has been used before, and it is credible that it is being considered for further use	Tactic has been used in the past, and a similar attack is planned
Threat Potential	Very Low	Low	Medium	High	Very High

3.9 Vulnerability determination

A vulnerability is defined as any weakness, flaw or condition that can be exploited for the successful realization of a potential threat against a transit system. As the threat environment is ever-changing, vulnerabilities to different threats and attack methods may also change. Transit agencies should constantly review their threats and vulnerabilities to ensure that they are addressing current trends.

Vulnerability conditions can be classified into two types: physical and procedural. A physical vulnerability condition is an actual physical deficiency, flaw or absence of physical measures designed to deter, detect, delay and/or respond against a breach or unauthorized access to a physical asset such as a stop or station. A procedural vulnerability condition relates to the existence, implementation, legality and oversight of policies

and procedures, which are designed to deter, detect, delay, respond or recover against a breach or unauthorized access to a physical asset.

The successful execution of a threat is dependent upon the presence of either a physical or procedural vulnerability, or both. By identifying the physical and procedural conditions that contribute to a certain threat, it is possible to start developing mitigation strategies to address the vulnerability and therefore reduce the likelihood and/or consequences of a successful attack. In general, vulnerability conditions allow access to an asset in order to be attacked.

Table 7 defines levels of vulnerability used in a vulnerability determination. In an existing system, the system would be reviewed with the criteria as stated. In a new system, consideration is given to planned or designed mitigations.

TABLE 7
Transportation System Vulnerability Determination

Vulnerability Level	Assessment Criteria
Very High	• Advanced physical and procedural mitigation measures are nonexistent or not planned for. • Existing or planned mitigation measures are inadequate and will likely fail to deter, detect, delay, respond to and recover from a security risk. • No security awareness culture present. • There are no business or operations contingencies in place to manage security events and recover. Severe disruptions are likely.
High	• Some mitigation measures are present or planned but are ineffective at deterring, detecting, delaying or responding to advanced security risks. • More than 50% of existing mitigation measures are likely to fail to deter, detect, delay or respond to a basic security risk. • No security exercises performed or planned. • Few contingencies/plans are in place for business and operations recovery. Significant disruptions likely.
Moderate	• 50% of advanced physical and procedural mitigation measures are effective, with remaining measures likely to fail to deter, detect, delay or respond to a security risk. • Existing mitigation measures are capable of deterring, detecting, delaying and responding to basic security risks. • Exercise program exists, and exercises are performed for select areas. • Basic security awareness culture exists. • Contingencies/plans are in place across most but not all key areas of business and operations but require improvement. Disruptions are likely.
Low	• 50% to 80% of advanced physical and procedural mitigation measures are effective, but some improvements are required. • Existing mitigation measures are capable of deterring, detecting, delaying and responding to basic security risks. • Procedures and evidence of audit and review of existing security measures. • Exercise program exists and exercises are performed for select areas. • Cultivation of security awareness culture is a management priority. • Business and operations contingencies are in place for all key areas to manage security events and recovery.

TABLE 7
Transportation System Vulnerability Determination

Vulnerability Level	Assessment Criteria
Very Low	• 80% or higher effectiveness of advanced mitigation measures to deter, detect, delay and respond to security risks, and measures are sustainable. • Procedures and evidence (records) of audit and review of existing controls. • Exercise program exists, and exercises are performed for select areas. • Security awareness culture is integrated into all business activities. • Comprehensive contingency plans in place across entire business and operations to manage most identified disruptions.

3.9.1 Likelihood assessment

Likelihood is the combination of threat, explained in **Table 5**, and vulnerability, illustrated in **Table 7**. **Table 8** describes how the combination results in a likelihood rating of the threat being realized.

TABLE 8
Likelihood Determination (Threat × Vulnerability)

Threat	Vulnerability				
	Very High	**High**	**Moderate**	**Low**	**Very Low**
Very High	Almost Certain A	Almost Certain A	Highly Likely B	Likely C	Likely **C**
High	Almost Certain A	Highly Likely B	Highly Likely B	Likely C	Possible D
Medium	Highly Likely B	Likely C	Likely C	Possible D	Possible D
Low	Likely C	Likely C	Possible D	Possible D	Remote E
Very Low	Possible D	Possible D	Possible D	Remote E	Remote E

Explanation of the likelihood ratings is included in **Table 9**.

TABLE 9
Likelihood Characteristics

Likelihood Rating	Likelihood Characteristics
Almost Certain A	Vulnerability exists, and threat is proven and demonstrated. Threat realization can be expected to occur during the system's operational phases.
Highly Likely B	Vulnerability exists, and threat is proven, though it may not be demonstrated. Threat realization may be expected during the system's operational phases.
Likely C	Some vulnerability exists and threat has some resource, experience and skill, though it may not be demonstrated. Threat realization may occur during the system's operational phases.
Possible D	Limited vulnerability, and threat may be under-resourced or lack experience and skill; should not occur during the system's operational phases.
Remote E	Limited vulnerability exists or threat has not been proven or demonstrated; not expected during the system's operational phases.

3.10 Consequence determination

Consequence (or severity), detailed in **Table 10**, is the assessed impact of a successful threat against a specific asset, the system or the network. Consequence is measured by the level of impact on primary areas of people, equipment and service, and by the impact upon the secondary areas of finance and reputation. It is critical that transit or rail agencies adjust the severity impacts to reflect their system and not adopt this matrix without evaluation and modification of the consequences to reflect their environment. Each category should be reviewed and assessed to ensure that they reflect the true severity to the transit or rail agency; otherwise, the final risk assessment process will be skewed and not produce results to frame the appropriate security risk for that agency.

In the examples below in the Financial column, the estimated loss of $5 million listed as a catastrophic loss might be appropriate for a midsized to large transit system but might not make sense for a small bus agency.

- **Example 1:**
  - In a rail agency with 50 railcars, the loss of a single railcar (~$1 million) might not critically impact the service or financial capability of the agency.
  - The loss of a single railcar (~$1 million) in a small agency that has only four railcars to provide service might be catastrophic if it impacted the ability to deliver service or if it could not afford to replace the railcar.
- **Example 2:**
  - In a small bus agency with infrequent service and few bus lines, operating in a small town, an assault resulting in a death might be catastrophic to the system.
  - For a large agency with multiple modes, running frequent service in a busy urban area, it might be more tolerable to experience a passenger fatality.

Particular attention should be paid to the bolded elements, as they are the most scalable components.

TABLE 10
Consequence Determinations

Consequence	Characteristics			
	People	Equipment/Services	Financial	Reputational
Catastrophic 1	**Several deaths** and/or numerous severe physical or psychological injuries	Total loss of equipment or system interruption, requiring **months** to repair	Estimated losses from the incident in excess of **$5 million**	Ongoing **international** media coverage, irreparable reputational damage, government intervention lasting **weeks or months**
Significant 2	**Low number of deaths** and/or severely physically or psychologically injured	Significant loss of equipment or system interruption, requiring **weeks** to repair	Estimated losses from the incident in the range of **$500,000 to $5 million**	Prolonged media campaign, serious reputational damage, sustained government involvement lasting **days or weeks**
Moderate 3	**Minor injury** and possible serious physical or psychological injury	Some loss of equipment or system interruption, requiring **seven or fewer** days to repair	Estimated loss in the range of **$50,000 to $500,000**	Adverse media coverage, reputational damage, government involvement

TABLE 10
Consequence Determinations

Consequence	Characteristics			
	People	Equipment/Services	Financial	Reputational
Minor 4	**Possible** minor physical or psychological injury	Some loss of equipment, no system interruption, less than **24 hours** to repair	Estimated losses are relatively minor, in the range of **$1,000 to $49,999**	Local media coverage and some reputational damage
Low/Negligible 5	No physical or psychological injury	Minor damage to equipment no system interruption, no immediate repair necessary	Estimated losses from the incident are likely less than **$1,000**	No adverse media coverage or reputational damage

3.11 Security risk rating determination

The security risk rating is the combination of likelihood and consequence. The initial risk rating applies threats against identified assets, using credible scenarios prior to considering controls or mitigations. The scenario process is discussed further in Section 3.8. The initial risk rating assumes that there is no additional risk mitigation applied. After mitigations or controls are considered, the residual risk is assessed again to determine if it will be acceptable or tolerable to the agency. **Table 11** shows the matrix to assess security risk using the identified likelihood and consequences previously discussed.

TABLE 11
Security Risk Matrix (Likelihood × Consequence)

Potential Consequences or Severity	Likelihood				
	Almost Certain A	Highly Likely B	Likely C	Possible D	Remote E
Catastrophic 1	Very High 1A	Very High 1B	High 1C	High 1D	Moderate 1E
Significant 2	Very High 2A	High 2B	High 2C	Moderate 2D	Moderate 2E
Moderate 3	High 3A	High 3B	Moderate 3C	Moderate 3D	Low 3E
Minor 4	Moderate 4A	Moderate 4B	Moderate 4C	Low 4D	Very Low 4E
Low/Negligible 5	Low 5A	Low 5B	Low 5C	Very Low 5D	Very Low 5E

Once the initial risk rating is determined for each scenario (security risk to asset), the risk index definitions (**Table 12**) define the actions required to determine and prioritize the resources and financial justification for risk treatment. Initial risk is the risk rating before the application of additional mitigations. The "Action Required" portion of the table should be modified to reflect a specific transit agency decision-making process. If there are certain levels of authority, such as the CEO or GM, who are part of the decision-making process or risk-acceptance process, they should be indicated as part of the "Action Required" column.

TABLE 12
Security Risk Action Definitions

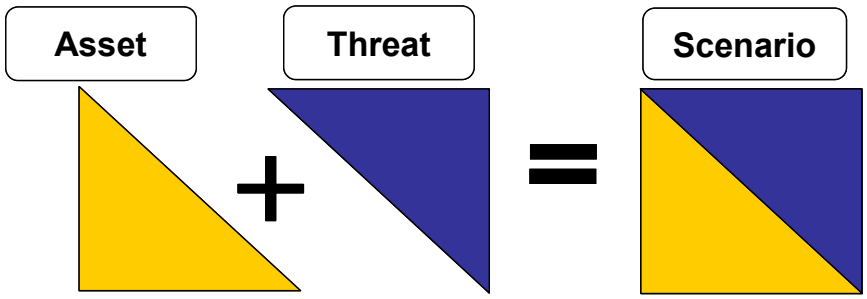
Risk Index	Risk Rating	Action Required
1A, 1B, 2A	**Very High**	Risk must be immediately mitigated and constantly monitored.
1C, 1D, 2B, 2C, 3A, 3B	**High**	Risk must be treated and constantly monitored.
1E, 2D, 2E, 3C, 3D, 4A, 4B, 4C	**Moderate**	Risk should be managed and reduction strategies implemented.
3E, 4D, 5A, 5B, 5C	**Low**	Risk may be accepted after a risk review.
4E, 5D, 5E	**Very Low**	Risk would normally not be treated.

Note: The cells can be ranked numerically to allow for priority within a risk rating category. Decisions based on priority should be made with full understanding about how the priority rating was achieved.

3.12 Threat scenarios

The security risk methodology is applied by using threat scenarios. A threat scenario pairs a specific threat against an identified asset. Examples might include an IED in a transit station or graffiti on a transit bus.

FIGURE 3
Threat Scenario Development



By pairing assets with threats, the vulnerabilities of that specific asset to the threat can be assessed. Once a transit system has identified threat scenarios relevant to its operations, the security risk can be evaluated: Determine the level of threat against an asset, determine how vulnerable the asset is, evaluate the likelihood that the asset will be attacked or harmed, and estimate the consequences of that action.

3.13 Example application

For illustration purposes, applications of the Security Risk Assessment process are provided in Appendix A. The example threat scenarios are graffiti of a transit bus or railcar and an active attacker on a railcar.

4. Risk treatment

Risk mitigations vary in their impact to security risk. Vulnerabilities can be resolved by deciding to either assume the risk associated with the threat/vulnerability or to eliminate or control the vulnerability. Most transit/rail systems do not have the ability to mitigate the threats, as these are not specific to public transportation but are rather societal, national or international. For most agencies, mitigations are applied to manage a security vulnerability resulting in an acceptable level of risk. The development of security mitigations should be coordinated with the safety group to ensure that the proposed mitigations will not introduce new safety hazards or exacerbate existing safety hazards.

4.1 Order of precedence

Mitigations should be applied in the following order of precedence, listed from most effective mitigations at the top of the list to least effective at the bottom:

- **Avoidance** (e.g., driverless systems avoid operator assaults)
- **Elimination** (e.g., eliminate cash payments for another fare system)
- **Substitution** (e.g., substitute high-security fence for a chain-link fence)
- **Engineering controls** (e.g., install access control)
- **Warnings** (e.g., signage)
- **Administrative controls** (e.g., Operations and Maintenance procedures)
- **Personal protective equipment and guards** (e.g., vests, Tasers)

There are a number of security measures and principles that can be applied to address asset and system vulnerability and consequence. To ensure that a robust and effective security outcome is delivered, measures must be complementary and offer sufficient redundancy should one or another completely or partially fail. The mitigation measures offered within this section are not the full extent of risk treatment options available but provide insight into protective security measures and three sound principles that are widely and successfully adopted for risk management within and outside of the transport environment:

- Crime Prevention Through Environmental Design (CPTED)
- layered security
- scalability

4.1.1 Crime Prevention Through Environmental Design

CPTED is a natural approach to crime prevention and differs from traditional approaches by placing emphasis on human activities and how they become exposed to crime. The National Crime Prevention Institute defines CPTED as a tool in creating safer environments: “The proper design and effective use of the built environment can lead to a reduction in the fear and incidence of crime, and an improvement in the quality of life.”

CPTED offers a holistic approach based on sociology, psychology and ecology of crime, as well as environmental criminology, criminal justice and architecture. The CPTED principles are applied to a physical environment or structure to reduce opportunities for violence and crime in a community and have the result of making people feel safer. It is based on the principle that most criminals decide to commit crimes based on opportunity that is inherent in how human space is designed or being used.

CPTED differs from procedural and physical security by placing emphasis on natural strategies. Natural strategies are aimed at integrating and incorporating behavior management into the design of human activity and physical resources.

The CPTED principles include the following:

- **Natural surveillance.** The design of an environment with clear sight lines to maximize visibility and observation. This includes the placement of physical features and activities to create a perception that individuals are under observation.
- **Natural access control.** Controlling access to a site through the strategic design of streets, sidewalks, building entrances and landscaping.

- **Territorial reinforcement.** The use of physical attributes that express ownership and notify users and non-users of the boundaries of a space or facility.
- **Maintenance and activity support.** Care and upkeep demonstrates ownership and intolerance for disorder. Encouraging appropriate activities preserves the intended use of the space.

Reference APTA's recommended practice "Crime Prevention Through Environmental Design (CPTED) for Transit Facilities" for further information about CPTED.

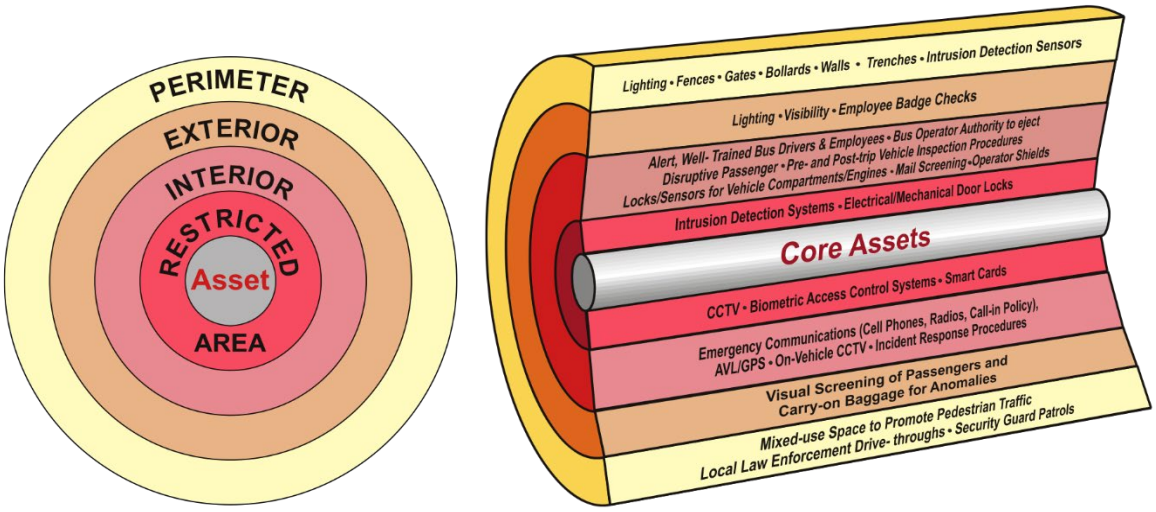
4.1.2 Layered security

Security measures that occur at several different levels or "layers" throughout a system, and at each facility, provide greater redundancy and defense-in-depth protection for assets and the system. The concept of layered protection recommends placing the most critical or vulnerable asset in the center of concentric levels of increasingly stringent security measures, as depicted in **Figure 4**. This allows multiple opportunities for thwarting or disrupting terrorist activities and is a key aspect of an effective security management strategy.

Some measures offer active defense such as highly visible security forces and physical security measures. These active defense mitigation measures aim to reduce the likelihood of an attack by limiting and preventing threat actors from being able to carry out their threat "attack sequence" of target selection, surveillance, planning, rehearsal, execution, escape and evasion. Additionally, these controls may see threat actors switch to a more lightly defended target, requiring constant and frequent vulnerability analysis by operators. The integration of CPTED supports the outcomes and efficiency of the layered security approach by causing threat actors to alter their behavior to suit the CPTED environment.

> **NOTE:** It is believed that terrorist groups commenced selecting softer, less protected transport systems due to hardening of government buildings and establishments. See Intelligence and Security Committee, "Report into the London Terrorist Attacks on 7 July 2005," page 26, "Targeting Transport Networks."

FIGURE 4
Layering Used to Protect Core/Critical Assets



An example of layered security exists in the placement of key assets and functions, such as where an Operations Control Center (OCC) should be placed within a complex. Positioning the OCC adjacent to public access areas may not offer the redundancy that exists with asset protection offered through layered security.

Instead the OCC should be located further within a building to limit penetration by offering redundancy through many layered security elements.

An important tool that determines the effectiveness of a layered security outcome and achieving security management goals is assessment through the contribution that the individual and collective protective security measures or mitigations offer to the security environment. The effectiveness of layered security is assessed by the ability of the measure to offer deterrence, delay, detection, response and recovery qualities, with some measures offering more than one quality. Using **Figure 4** as a reference, security force presence offers deterrence, detection and response qualities. As with lighting and video surveillance, both measures offer deterrence and detection properties.

4.1.3 Scalability

The selection of mitigations within the system should be considered in the context of providing daily sufficiency and supporting scalability during periods of elevated threat. During the design/planning phase of a project, the selection of day-to-day "baseline measures" that offer full scalability during periods of elevated threat and then subsequent reduction of threat is important for the continuing efficiency of the transit system.

4.1.4 Mitigations

Mitigations are the measures applied to reduce the overall security risk. Design or physical mitigations are designed or retrofitted in to either reduce the vulnerability of the system to threat or, possibly, reduce the consequence of a realized threat. These would include mitigations like surveillance systems, access control, fencing barriers and intrusion detection. These are often paired with operational or procedural mitigations such as plans and procedures, maintenance protocols, or policing and security personnel. Mitigations may impact the vulnerability, the consequence or both, but there should be a mindful review of exactly how mitigations impact the elements of the assessment.

There are many security mitigations that can be applied to address asset and system vulnerability and consequence. To ensure that a robust and effective security outcome is delivered, measures must be complementary and offer sufficient redundancy should one or another completely or partially fail. The goal is to apply the right mitigations as part of a layered approach to security to reduce risk to an acceptable level.

Mitigations have various attributes to how they impact security. Some of these are represented in **Table 13** for reference. The applicability of the individual security measures are mapped against the following:

- Deter (D)
- Delay (D)
- Detect (D)
- Respond (R)
- Recover (R)

TABLE 13
Security Mitigations

SECURITY MEASURE	APPLICABILITY				
	Deter	Delay	Detect	Respond	Recover
Physical Controls					
Signage	Yes	No	No	No	No
Perimeter and internal barriers (CPTED)	Yes	Yes	No	No	No
Projectile shields	Yes	Yes	Partial	No	No
Proximity to local traffic (pedestrian and vehicle)	Yes	Partial	Partial	Partial	No
Open lines of sight (CPTED, absence of building or terrain cover)	Yes	No	Yes	No	No
Area lighting conditions (CPTED)	Yes	No	Yes	No	No
Building materials and design (CPTED)	Partial	Yes	No	No	No
Vehicle control and calming measures (CPTED)	Yes	Yes	Yes	No	No
Security buffer zones (CPTED)	Partial	Yes	No	Yes	No
Construction codes (CPTED)	Partial	Yes	No	No	No
Mail screening	Partial	No	Yes	No	No
Policy/Process Controls					
Employee awareness program	Yes	No	Yes	No	No
Personnel screening	Partial	No	Yes	No	Partial
Entry searches	Yes	No	Yes	No	No
Policy and Process					
Employee termination procedure	No	No	No	Yes	No
Staff training	Yes	Yes	Yes	Yes	Yes
Ethical frameworks and monitoring	Yes	Partial	Yes	No	No
Identity cards	Partial	No	Yes	No	No
Law enforcement response	Partial	No	No	Yes	No
Uniformed security patrols	Yes	Yes	Yes	Yes	Yes
Covert security patrols	Partial	Yes	Yes	Yes	No
Management supervision	Yes	Yes	Yes	No	No
Risk management	Partial	Partial	Partial	Partial	Partial
Inventory control systems	Yes	Yes	Yes	No	No
Internal audit and other assurance systems	Partial	Partial	Partial	Partial	Partial
Lock-key practices	No	Yes	No	No	No
Housekeeping	No	Partial	Yes	Partial	No
Evacuation plans	No	No	No	Yes	No
Process design	Yes	Yes	Yes	Yes	Yes
Authorization and delegation governance	Yes	Yes	Yes	No	No

TABLE 13
Security Mitigations

SECURITY MEASURE	APPLICABILITY				
	Deter	Delay	Detect	Respond	Recover
Policy framework	Partial	Partial	Partial	Partial	Partial
Emergency management planning	No	No	No	Yes	Partial
Business continuity management	No	No	No	Yes	Yes
Corporate governance	Yes	Yes	Yes	Partial	Partial
Document control	No	Yes	Partial	Partial	No
Communications and public affairs policies and practices	No	No	Partial	No	No
Prior publicized responses to security breaches	Yes	No	No	No	No
Security access systems	Yes	Yes	Partial	No	No
Intrusion detection and alarms	Yes	No	Yes	No	No
Password and encryption keys	Yes	Yes	No	No	No
Firewalls	Yes	Yes	Partial	No	No
Surveillance capability	Yes	No	Yes	No	No
Systems penetration testing	No	Yes	Yes	Yes	No
Panic alarms	No	No	No	Yes	No

5. Documentation

Security risk assessment worksheets are used to document the security assessment. These may take many forms, and the actual format is inconsequential, as long as the information is tracked and can be managed. **Figure 5** illustrates one example of a TVA format. A blank form is included as Appendix B.

FIGURE 5
Sample TVA Worksheet

Identification Number	Asset	Threat Type/Event	Threat Rating	Vulnerability Rating	Likelihood Index (Threat/Vulnerability)	Potential Effect	Consequence Index	Initial Risk Rating (Likelihood/Consequence)	Potential Mitigation Measures	Residual Risk Rating
D-7	Bus	**Armed Attack** (Armed attack on a bus)	Medium	Very High	B Highly Likely	Economic disruption to system and adjacent facilities	2 Significant	2B HIGH	CCTV coverage of BRT vehicle	2D MOD
									Operator security awareness training	
									Public security awareness program	
						Damage to equipment and facilities			Training of uniform security force/police on threat environment and transportation security	
						Death and/or injury			Implementation of suspicious activity reporting and communication procedures	
						Operational disruption			Radom, persistent, and visible inspection and patrol of buses by operators or security	
						Major reputational damage			Random visible police presence	

6. Security assurance

Once agreement is reached and a determination has been made to implement a mitigation, agencies should assign a responsible party for the implementation of the mitigation. After implementation is complete and verification evidence has been confirmed, the mitigation should be verified to ensure that it has been incorporated correctly. This can be done through a verification process or other means but should be documented as complete. The verification process could include use of a security log or database to track ongoing actions and closed mitigation items. Completed verification should be communicated to appropriate parties.

There should be an ongoing examination to confirm that the selected mitigations stay effective and manage the system's vulnerabilities. This can be part of an audit or review process where vulnerabilities and the associated mitigations are reviewed and evaluated for effectiveness. This is consistent with both the requirements for the Safety and Security Certification process and the Safety Management System.

Related APTA standards

APTA SS-SIS-RP-007-10, "Crime Prevention Through Environmental Design (CPTED) for Transit Facilities"

References

Atlas, R.I., "21st Century Security and CPTED: Designing for critical infrastructure protection and crime prevention," 2nd Edition, CRC Press, Taylor & Francis Group, Boca Raton, Florida, 2013.

American Association of State Highway and Transportation Officials (AASHTO), "A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection," 2016. transportationops.org/research/guide-highway-vulnerability-assessment-critical-asset-identification-and-protection

ASIS International, "International Glossary of Security Terms." asisonline.org/publications--resources/standards--guidelines/orm/annex-g/

Department of Homeland Security (DHS), National Terrorism Advisory System (NTAS), 2011. https://www.dhs.gov/national-terrorism-advisory-system

Department of Homeland Security (DHS), National Infrastructure Protection Plan (NIPP), 2009. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2009-508.pdf

Department of Homeland Security (DHS), "DHS Risk Lexicon," September 2010. dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

DHS/Transportation Security Administration (TSA), "Sensitive Security Information Program, SSI Training for Surface Transportation Stakeholders."

Federal Emergency Management Agency (FEMA), "Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks," FEMA 430, 2007. https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf

Federal Emergency Management Agency (FEMA), FEMA 452 "A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings," 2005. https://www.wbdg.org/ffc/dhs/criteria/fema-452

Federal Transit Administration (FTA), "The Public Transportation System Security and Emergency Preparedness Planning Guide," 2003. transit.dot.gov/sites/fta.dot.gov/files/docs/PlanningGuide.pdf

Federal Transit Administration (FTA), "An Introduction to All-Hazards Preparedness for Transit Agencies," 2010. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/All_hazards.pdf

Federal Transit Administration (FTA), "Public Transportation System Security and Emergency Preparedness Planning Guide," 2003. transit.dot.gov/sites/fta.dot.gov/files/docs/PlanningGuide.pdf

Federal Transit Administration (FTA), "Sensitive Security Information (SSI): Designation, Markings and Control," February 2020. transit.dot.gov/oversight-policy-areas/sensitive-security-information-ssi-designation-markings-and-control-march

State Government of Victoria (Australia) Department of Transport, "Security Risk Assessment for Transport Operators," Department of Transport, Melbourne, Australia, 2012.

Department of Homeland Security, Transportation Security Administration, "SSI Best Practices Guide for Non-DHS Employees and Contractors." https://www.tsa.gov/sites/default/files/ssi_best_practices_guide_for_non-dhs_employees.pdf

Transportation Security Administration (TSA)/Federal Transit Administration (FTA), "Security and Emergency Management Action Items for Transit Agencies." hsdl.org/?view&did=773635

Transportation Research Board of the National Academies, "Security 101: A Physical and Cybersecurity Primer for Transportation Agencies," 2020. trb.org/NCHRP/Blurbs/179516.aspx

Wilson, J.Q., and Kelling, G.L., "Broken Windows: The police and neighborhood safety," The Atlantic, March 1982. theatlantic.com/magazine/archive/1982/03/broken-windows/304465/5/

Definitions

broken windows theory: A crime theory that links physical and social disorder and incivility within a community to subsequent occurrences of serious crime.

consequence: The level, duration and nature of loss from an unfavorable event.

detect: The act of discovering an attempt (successful or unsuccessful) to breach a secured perimeter (such as scaling a fence, opening a locked window or entering an area without authorization).

deter: To discourage or prevent someone from doing something.

risk: The likelihood of the occurrence of an unfavorable event that leads to catastrophic losses (fatalities, injuries, damage or business interruption). The three factors of risk are threat, vulnerability and consequence.

recovery: The ability to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption.

response: Employees, guards or law enforcement representatives who deploy to investigate a detection event or interdict an intruder or trespasser.

Security Risk Assessment: An assessment intended to evaluate a transit/rail system's susceptibility to security threats and to identify vulnerabilities and potential consequences.

severity: See *consequence*.

target: An object, background or reflector at which something (i.e., a threat) is aimed.

threat: A human-made act that harms or has the potential to harm life, information, operations, the environment and/or property.

threat actor: The person or entity responsible for a security event or incident.

vulnerability: A physical feature or operational attribute that renders a station or stop open to exploitation or susceptible to a given hazard or threat. Vulnerabilities may be associated with physical, cyber or human factors.

Abbreviations and acronyms

AASHTO American Association of State Highway and Transportation Officials
ALARP as low as reasonably practicable
BIPS Buildings and Infrastructure Protection Series
CFR Code of Federal Regulations
CPTED Crime Prevention Through Environmental Design
DHS Department of Homeland Security
FEMA Federal Emergency Management Agency
FOIA Freedom of Information Act
FTA Federal Transit Administration
HVE homegrown violent extremists
IED improvised explosive device
IID improvised incendiary device
IRVS Integrated Rapid Visual Screening Series
ISAC Information Sharing and Analysis Centers
NATSA North American Transportation Services Association
NIPP National Infrastructure Protection Plan
NIST National Institute of Standards and Technology
NTAS National Terrorism Advisory System
NTI National Transit Institute
PBIED person-borne improvised explosive device
PT-RAM Public Transit Risk Assessment Methodology
SPR Stakeholder Preparedness Review
SSI Sensitive Security Information
THIRA Threat and Hazard Identification and Risk Assessment
TSA Transportation Security Administration
TVA Threat and Vulnerability Assessment
UAS unmanned aircraft system
VBIED vehicle-borne improvised explosive device

Summary of document changes

- Bullet points xx

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	CEO Review Approval	Policy & Planning Approval	Publish Date
First published	July 24, 2020	Sept. 9, 2020	Oct. 23, 2020	Dec. 22, 2020	March 23, 2021
First revision	—	—	—	—	—

Appendix A: Example applications of methodology

Example 1: Graffiti on transit buses and railcars

Threat rating

Graffiti on transit buses or railcars is widely found and generally does not vary substantially from agency to agency. For most systems, graffiti would be assessed as a **Very High** threat based on the threat matrix. Transit agencies that do not run in cities or environments that experience graffiti should rate this threat as they are experiencing it. This might be reflective of a lower level of intent, rather than a lower capability.

Intent	Capability				
	Similar exploit has been used	Operational capability confirmed by credible evidence	Some evidence that operational capability exists; not confirmed	No evidence of operational capability but feasibility confirmed	No evidence and even feasibility unconfirmed
Tactic has been used in the past, and a similar attack may be planned	**Very High**	Very High	High	Medium	Low
Tactic has been used before, and it is credible that it is being considered for further use	Very High	High	High	Medium	Low
Tactic has not been used before but is under consideration	High	High	Medium	Medium	Low
Tactic has not been used before, but it may be under consideration	Medium	Medium	Medium	Low	Very Low
Tactic has not been used before and is not known to be under consideration	Low	Low	Low	Very Low	Very Low

Vulnerability rating

Transit and rail agencies, as open access environments, are very vulnerable to some types of criminal enterprise, including graffiti. Even with levels of security, writing with a marker on a bus or train or on the walls of a station or stop is difficult to prevent. For this reason, vulnerability to graffiti on transit buses or railcars is rated as **High**.

Vulnerability Level	Assessment Criteria
High	• Some mitigation measures are present or planned, but are ineffective at deterring, detecting, delaying or responding to advanced security risks. • More than 50% of existing mitigation measures are likely to fail to deter, detect, delay or respond to a basic security risk. • No security exercises performed or planned. • Few contingencies/plans are in place for business and operations recovery. Significant disruptions likely.

Likelihood determination

Using the **Very High** rating for the threat of graffiti on transit buses or railcars, with a **High** vulnerability rating of graffiti on transit buses or railcars , rates this as an **Almost Certain** likelihood rating for graffiti on transit buses or railcars.

Threat	Vulnerability				
	Very High	**High**	**Moderate**	**Low**	**Very Low**
Very High	Almost Certain A	**Almost Certain** **A**	Highly Likely B	Likely C	Likely **C**
High	Almost Certain A	Highly Likely B	Highly Likely B	Likely C	Possible D
Medium	Highly Likely B	Likely C	Likely C	Possible D	Possible D
Low	Likely C	Likely C	Possible D	Possible D	Remote E
Very Low	Possible D	Possible D	Possible D	Remote E	Remote E

Consequence rating

The next step in the process is to determine the criticality or consequence of graffiti. The impact of graffiti isn't one that involves harm to people, impacts service or has other major impacts. Graffiti on transit buses or railcars would be rated as **Low/Negligible** with these consequence definitions.

Consequence	Characteristics			
	People	**Equipment/Services**	**Financial**	**Reputational**
Low/Negligible **5**	No physical or psychological injury	Minor damage to equipment, no system interruption, no immediate repair necessary	Estimated losses from the incident are likely less than **$1,000**	No adverse media coverage or reputational damage

Security risk rating

After working through the rating process, using an **Almost Certain** likelihood and a **Low/Negligible** consequence indicates that graffiti on transit buses or railcars is a **Low** security risk.

Potential Consequences or Severity	Likelihood				
	Almost Certain A	**Highly Likely B**	**Likely C**	**Possible D**	**Remote E**
Catastrophic 1	Very High 1A	Very High 1B	High 1C	High 1D	Moderate 1E
Significant 2	Very High 2A	High 2B	High 2C	Moderate 2D	Moderate 2E
Moderate 3	High 3A	High 3B	Moderate 3C	Moderate 3D	Low 3E
Minor 4	Moderate 4A	Moderate 4B	Moderate 4C	Low 4D	Very Low 4E
Low/Negligible 5	**Low 5A**	Low 5B	Low 5C	Very Low 5D	Very Low 5E

Example 2: Active attack on a railcar

Threat rating

Active assailant attacks occur sporadically in all types of environments, to include public transit systems. Assailants armed with firearms, knives and other weapons, may target public transit systems in pursuit of extremist agendas. While this threat affects all agencies, specific threats may vary based on locale. For most

systems, an active attack on a railcar would be assessed as a **Very High** threat based on the threat matrix, as adversaries have repeatedly demonstrated both the intent and capability.

Intent	Capability				
	Similar exploit has been used	Operational capability confirmed by credible evidence	Some evidence that operational capability exists; not confirmed	No evidence of operational capability but feasibility confirmed	No evidence and even feasibility unconfirmed
Tactic has been used in the past, and a similar attack may be planned	**Very High**	Very High	High	Medium	Low
Tactic has been used before, and it is credible that it is being considered for further use	Very High	High	High	Medium	Low
Tactic has not been used before but is under consideration	High	High	Medium	Medium	Low
Tactic has not been used before, but it may be under consideration	Medium	Medium	Medium	Low	Very Low
Tactic has not been used before and is not known to be under consideration	Low	Low	Low	Very Low	Very Low

Vulnerability rating

Transit agencies, as open access environments, are vulnerable to violent crime, including an active attack on a railcar. Prevention activities and protective measures, such as a visible security and law enforcement presence, may reduce vulnerability to active assailant attacks, though active attacks can be unpredictable and occur without warning. Vulnerability ratings for active assailant attacks may differ across agencies, as entities possess varying levels of prevention and protective measures. In this example, vulnerability to active attackers is rated as **Moderate**, as agencies may have executed prevention, protection and mitigation activities to reduce vulnerability to this threat.

Vulnerability Level	Assessment Criteria
Moderate	• 50% of advanced physical and procedural mitigation measures are effective, with remaining measures likely to fail to deter, detect, delay or respond to a security risk. • Existing mitigation measures are capable of deterring, detecting, delaying and responding to basic security risks. • Exercise program exists, and exercises are performed for select areas. • Basic security awareness culture exists. • Contingencies/plans are in place across most but not all key areas of business and operations but require improvement. Disruptions are likely.

Likelihood determination

Using the **Very High** threat rating and **Moderate** vulnerability rating, this active attack scenario has a **Highly Likely** likelihood rating.

Threat	Vulnerability				
	Very High	**High**	**Moderate**	**Low**	**Very Low**
Very High	Almost Certain A	Almost Certain A	**Highly Likely** **B**	Likely C	Likely **C**
High	Almost Certain A	Highly Likely B	Highly Likely B	Likely C	Possible D
Medium	Highly Likely B	Likely C	Likely C	Possible D	Possible D
Low	Likely C	Likely C	Possible D	Possible D	Remote E
Very Low	Possible D	Possible D	Possible D	Remote E	Remote E

Consequence rating

The next step in the process is to determine the criticality or consequence of an active attacker. The impact of an active attacker may vary based on the tactics and weaponry in use, but a successful active assailant attack would most likely harm people, damage equipment, impact service and cause other impacts. An active attack on a railcar may be rated as **Significant** with these consequence definitions.

Consequence	Characteristics			
	People	**Equipment/Services**	**Financial**	**Reputational**
Significant **2**	**Low number of deaths** and/or severely physically or psychologically injured	Significant loss of equipment or system interruption, requiring **weeks** to repair	Estimated losses from the incident in the range of **$500,000 to $5 million**	Prolonged media campaign, serious reputational damage, sustained government involvement lasting **days or weeks**

Security risk rating

After working through the rating process, a **Highly Likely** likelihood and a **Significant** consequence indicates that an active attack on a railcar is a **High** security risk.

Potential Consequences or Severity	Likelihood				
	Almost Certain A	**Highly Likely B**	**Likely C**	**Possible D**	**Remote E**
Catastrophic 1	Very High 1A	Very High 1B	High 1C	High 1D	Moderate 1E
Significant 2	Very High 2A	**High 2B**	High 2C	Moderate 2D	Moderate 2E
Moderate 3	High 3A	High 3B	Moderate 3C	Moderate 3D	Low 3E
Minor 4	Moderate 4A	Moderate 4B	Moderate 4C	Low 4D	Very Low 4E
Low/Negligible 5	Low 5A	Low 5B	Low 5C	Very Low 5D	Very Low 5E

Appendix B: Sample TVA tracking form

Threat, Vulnerability, and Consequence Form														
Identification Number	Asset	Threat Type/Event	Threat Rating	Vulnerability Condition		Vulnerability Rating	Likelihood Index (Threat/Vulnerability)	Potential Effect	Consequence Index	Initial Risk Rating (Likelihood/Consequence)	Potential Mitigation Measures	Residual Risk Rating	Verification & Validation		
				Procedural	Physical								Responsible Party	Reference/ Status	Acceptance of Resolution
A-1															
A-2															