Buildings and Infrastructure Protection Series

Integrated Rapid Visual Screening of Tunnels

BIPS 03/March 2011

Homeland Security

Science and Technology

Buildings and Infrastructure Protection Series

Integrated Rapid Visual Screening of Tunnels

BIPS 02/March 2011

Homeland Security

Science and Technology

This publication was produced by the Department of Homeland Security, Science and Technology Directorate, Infrastructure Protection and Disaster Management Division.

Foreword and Acknowledgments

Since the events of September 11, 2001, government officials, law enforcement, the design community, transportation specialists, and first responders have understood that the risk environment has changed and that the Nation's critical assets must be protected. The Department of Homeland Security (DHS) has identified transportation infrastructure as a Critical Infrastructure and Key Resource (CIKR) Sector.

DHS has sponsored the development of a methodology for assessing the risk and resilience of tunnels to terrorist attacks and selected natural hazards. The methodology, referred to as the integrated rapid visual screening (IRVS) for tunnels, was developed by the DHS Science and Technology Directorate (DHS S&T), Infrastructure Protection and Disaster Management Division, in partnership with the Risk Assessment Division of the Transportation Security Administration (TSA). TSA is currently adopting the IRVS of mass transit stations to enhance its risk assessment of transportation systems throughout the country. The following were also involved in the development and testing of the methodology for the IRVS of mass transit stations: Massachusetts Bay Transportation Authority; Port Authority of New York and New Jersey; and private-sector stakeholders involved in the design, operation, and management of critical infrastructure.

"Integrated" in IRVS indicates that the methodology includes the risk of both terrorist acts and natural hazards and an assessment of both risk and resiliency.

The result of an IRVS of tunnels is a quantifiable assessment of the risk of a given tunnel to a terrorist attack or natural disaster that leads to catastrophic losses (fatalities, injuries, damage, or business interruption) and a quantifiable assessment of the resiliency of the tunnel(ability to recovery from such an event).

Needs and Purpose

Transportation tunnels have been identified as an attractive target for terrorist attacks because of their accessibility and potential impact on human lives and economic activity. Numerous tunnels in the United States are located at critical chokepoints. A critical choke point is a point in the transportation network where many trip paths intersect to get through a geographic barrier.

The U.S. transportation system includes approximately 337 highway tunnels and 211 mass transit tunnels.

The U.S. transportation system includes approximately 337 highway tunnels and 211 mass transit tunnels, and many have limited alternative routes because of geographic constraints. Many transit tunnels are underwater. The loss of critical tunnels could result in hundreds or thousands of casualties, billions of dollars of direct reconstruction costs, and even greater socioeconomic costs. The downtime associated with an attack on a tunnel could range from days to years (FHWA, 2003).

There has not been a direct attack on a highway or mass transit tunnel in the United States, but terrorist plots involving tunnels have been discovered and thwarted. In 2006, U.S. authorities discovered a plot in the early planning stage to attack mass transit tunnels under New York's Hudson River (Hsu and Wright, 2006).

The loss of critical tunnels could result in hundreds or thousands of casualties, billions of dollars of direct reconstruction costs, and even greater socioeconomic costs.

Tunnels can receive collateral damage from attacks on other targets because of their underground or underwater location. For example, collateral damage from the attacks of September 11, 2001, rendered the Port Authority Trans-Hudson (PATH) commuter rail line unusable for 2 years. The PATH station and tunnel were connected to the World Trade Center towers via an underground concourse and shopping center. The collapse of the towers resulted in a partial collapse of several areas of the tunnel lining and led to flooding in certain areas. The rail line carried 67,000 passengers to Lower Manhattan every weekday (FHWA, 2003).

The goals of terrorists are to attract attention, disrupt the economy, create fear, and disrupt the social fabric. Selected targets may not have a pattern.

Terrorists may use methods that have been used before or they may use new methods. The possibility that new methods may be used complicates mitigation.

The primary purpose of the IRVS of tunnels is to rank the risk in a group of tunnels in a transportation system or region.

To better quantify, qualify, and mitigate the risks to mass transit systems, DHS S&T has dedicated resources to developing risk assessment and mitigation tools to protect tunnels and mass transit stations. The assessment of tunnels is described in this document, and the assessment of mass transit stations is described in the Integrated Rapid Visual Screening of Mass Transit Stations (DHS, 2011a).

The primary purpose of the IRVS of tunnels is to rank the risk in a group of tunnels in a transportation system or region. The results of an IRVS can also be used in infrastructure-specific risk assessments and higher level assessments of threats, consequences, and vulnerabilities.

This document is the manual for conducting an IRVS of tunnels and provides guidance in rating a tunnel's potential risk of and resiliency to terrorist attacks and selected natural disasters (fire and flooding).

Relationship of the IRVS of Tunnels to the Risk Management Series

The technical concepts and field application of the methodology are based on the Risk Management Series (RMS), a widely accepted series of publications that provide risk evaluation methods and design guidance for mitigating multi-hazard events. The design concepts from the RMS are represented in the IRVS methodology in the evaluation of favorable and unfavorable characteristics of a tunnel that influence the risk of the structure to specific threats.

Furthermore, the field application of the IRVS reflects the procedures for risk assessment outlined in several RMS publications. The series was developed by DHS's Federal Emergency Management Agency (FEMA) after the events of September 11, 2001. The IRVS methodology is drawn largely from the following three RMS publications:

- FEMA 426, *Reference Manual for the Protection of Buildings Against a Terrorist Attack* (DHS, 2011c)
- FEMA 452, *Risk Assessment, A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings* (FEMA, 2005)
- FEMA 455, *Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks* (FEMA 2009)

The differences between the rapid visual screening (RVS) described in FEMA 455 and the IRVS of tunnels described in this manual are:

- RVS is used to screen buildings, and IRVS is used to screen tunnels
- RVS focuses on the risk of terrorists acts, and IRVS focuses on both terrorist acts and selected natural hazards (fire and flooding)
- RVS focuses on risk, and IRVS focuses on both risk and resiliency

"Integrated" in IRVS indicates that the methodology includes the risk of both terrorist acts and natural hazards and an assessment of both risk and resiliency.

Relationship of the IRVS of Tunnels to the National Infrastructure Protection Plan

The IRVS methodology closely follows the general risk management framework and definitions identified in DHS's National Infrastructure Protection Plan (NIPP) (DHS, 2009b), including the Critical Infrastructure and Key Resources (CIKR) Sectors. The risk management framework in the NIPP involves scenario-based consequence and vulnerability estimates and an assessment of the likelihood that a postulated threat will occur. The IRVS is based in part on the NIPP's core criteria for risk assessments, as follows:

- **Documented** – This manual includes the types of information that are collected during the IRVS and how the information is synthesized to generate a risk and resiliency assessment. All assumptions, weighting factors, and subjective judgments are explained.
- **Reproducible** – The methodology has been tested to ensure that the results are reproducible.
- **Defensible** – The components of the methodology are integrated logically, and disciplines that are relevant to the methodology are incorporated appropriately (e.g., engineering, architecture, construction, emergency management, security). The methodology has been tested to ensure that the results are reproducible, and the results produced by the methodology have been validated.
- **Complete** – The methodology includes an assessment of consequences, threats, and vulnerabilities for every defined scenario and an assessment of the resiliency to postulated threats.

The NIPP includes the 18 CIKR Sectors that are identified in Homeland Security Presidential Directive 7. CIKR Sectors are the assets, systems,

and networks that provide similar functions to the economy, government, or society. The IRVS incorporates the 18 CIKR Sectors in the target density evaluation and includes all sectors in determining the threat of collateral damage from attacks on other targets.

"Integrated" in IRVS indicates that the methodology includes the risk of both terrorist acts and natural hazards and an assessment of both risk and resiliency.

Partnerships

DHS S&T and the Risk Assessment Division of the Transportation Security Administration worked in partnership to develop the IRVS methodology. The partners reviewed the factors involved in risk and resiliency scoring and conducted pilot and field studies of a variety of tunnels throughout the Nation. TSA plans to use the tool to enhance its risk assessment of transportation systems throughout the country. Equally important was the cooperation provided by the Metro Boston Transportation Agency and the Port Authority of New York and New Jersey. Both agencies provided DHS with invaluable information, including how the methodology could realistically be expected to be used, which helped determine the scope of the methodology.

Intended Audience

This manual is intended for both technical and stakeholder audiences. Technical audiences include potential screeners and personnel who are knowledgeable about tunnels but who may not have a high level of expertise. Stakeholders include owners, operators, and decision-makers involved in the planning and maintenance of tunnels.

The intended audience includes:

- Transportation authorities
- City, county, and State officials
- Emergency managers
- Law enforcement personnel
- Facility managers
- Security consultants
- Engineers, architects, and other design professionals

This publication has been produced by the Department of Homeland Security (DHS) Science and Technology (S&T), Infrastructure Protection and Disaster Management Division (IDD).

Acknowledgments

Project Officer

Milagros Kennett, Architect/Program Manager, Department of Homeland Security, Science and Technology Directorate, Infrastructure Protection and Disaster Management Division

Authors

Mohammed Ettouney, Weidlinger Associates, Inc.

Stephen Hughes, URS Group, Inc.

Richard F. Walker Jr., URS Group, Inc.

Eric Letvin, National Institute of Standards and Technology

Software Developer

Terrence Ryan, Raytheon UTD, Inc.

External Review Committee

Nanne Davis Eliot, National Institute of Building Sciences

Dean Fajerski, Transportation Security Administration

Robert Melan, Transportation Security Administration

Christopher McKay, Transportation Security Administration

Paul Martin, New York State, Department of State

Daniel O'Brien, New York State, State Emergency Management Office

Christopher Arnold, Building Systems Development, Inc.

Andrea Schultz, Department of Homeland Security

Gwainevere Hess, Department of Homeland Security

Artie Mendez, City of New York Police Department

Michael Chipley, The PMC Group, LLC

Philip Schneider, National Institute of Building Sciences

Diana Burke, URS Group, Inc.

Pilot Test Partners

Lewis Best, Massachusetts Bay Transportation Authority Transit Police

John Joyce, Greater Cleveland Regional Transit Authority Police

Willie McCuller, Metro Transit St. Louis

David Warrington, Port Authority of New York and New Jersey

Sharlene Salazar, Port Authority of New York and New Jersey

Brian Lacey, Port Authority of New York and New Jersey

Adam Hutter, Department of Homeland Security, Science and Technology Directorate

Graphic Designer

Wanda L. Rizer, Design4Impact

This publication was prepared under contract to DHS. It will be revised periodically, and comments and feedback to improve future editions are welcome. Please send comments and feedback to bips@dhs.gov.

Table of Contents

Will remake TOC AFTER this round of edits as I suspect there will be changes to sections.

Tables

Figures

1

Overview

In this chapter:

The methodology, referred to as integrated rapid visual screening (IRVS), can be used by transit agencies to assess a transit system that includes buildings, tunnels, and mass transit stations.

In response to the need to improve the protection of the Nation's critical assets, the Department of Homeland Security's Science and Technology Directorate (DHS S&T) has initiated the development of a methodology for assessing the risk and resilience of buildings, tunnels, and mass transit stations to terrorist attacks and natural disasters that result in catastrophic losses (fatalities, injuries, damage, or business interruption). Resilience is the ability of a facility to recover from a terrorist attack or natural hazard (see Section 1.3.2 for more information on resilience).

The methodology, referred to as integrated rapid visual screening (IRVS), can be used by transit agencies to assess a transit system that includes buildings, tunnels, and mass transit stations.

1.1 IRVS Family

The IRVS of Tunnels (described in this Manual) is just one type of infrastructure in the IRVS family developed by DHS S&T. Infrastructure-specific IRVS assessments have also been developed for buildings and mass transit stations. The IRVS family is described in the following documents published by DHS S&T:

- BIPS 02, Integrated Rapid Visual Screening of Mass Transit Stations (DHS, 2011)
- BIPS 03, Integrated Rapid Visual Screening of Tunnels (DHS, 2011b)
- BIPS 04, Integrated Rapid Visual Screening of Buildings (DHS, 2011a)

Each IRVS assessment is tailored to evaluate the unique characteristics of the infrastructure type that influence the risk and resiliency. The IRVS family can be used in conjunction to evaluate a system that may include mass transit stations, tunnels, and buildings.

1.2 Validation

DHS S&T validated the IRVS through alpha and beta testing in partnership with the Transportation Security Administration (TSA) and in cooperation with Massachusetts Bay Transportation Authority (MBTA) and Port Authority of New York & New Jersey (PANYNJ). One objective of the alpha and beta testing was to evaluate or determine the following:

- User-friendliness of the documentation and software
- Clarity of the description of the methodology
- Duration of a typical building evaluation by newly trained assessors
- Sensitivity of the scoring system (attribute weights) to various tunnel attributes
- Variation among scores for different tunnel types
- Consistency of results

A second objective of the testing was to collect data on a wide array of buildings with unique characteristics throughout the Nation.

The results of the alpha and beta testing were used as a basis for:

- Adding, deleting, and modifying tunnel characteristics
- Modifying the weighting factors for building attribute options

- Calibrating the tool to obtain accurate, consistent, and reasonable risk scores for each IRVS for different types of tunnels. Calibration of scoring includes the overall risk score and the scores for each threat scenario and the consequences rating, threat rating, and vulnerability rating.

The IRVS of MTS was validated in four of the largest mass transit systems in the United States: New York City, Washington D.C., Boston, Cleveland, and St. Louis. In addition, this manual was reviewed by TSA, MBTA, and PANYNJ.

DHS S&T is developing a design program that promotes high performance in resistance to hazard events, resilience, security, sustainability, and energy efficiency.

1.3 Risk and Resilience

The two objectives of the IRVS of Tunnels are to assess the risk and resilience of a tunnel to a terrorist attack or selected natural hazards (fire and flooding) and resilience to such an event.

1.3.1 Risk

Risk is the likelihood of the occurrence of an unfavorable event that leads to catastrophic losses (fatalities, injuries, damage, or business interruption). The three components of risk are consequences, threat, and vulnerability. Consequence is the level, duration, and nature of loss from an unfavorable event; threat is the threat of a manmade or natural unfavorable event with the potential to harm life, information, operations, the environment, and/or property; and vulnerability is defined as a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. See Section 2.5.2 for more information about consequences, threat, and vulnerability.

Risk is the likelihood of the occurrence of an unfavorable event that leads to catastrophic losses (fatalities, injuries, damage, or business interruption).

The three components of risk are consequences, threat, and vulnerability.

1.3.2 Resilience

Resilience is defined as "the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions" (DHS, 2009b)." Figure 1-1 shows an example of an asset's resilience after an event.

Resilience is defined as the effectiveness of protective measures to reduce the impact of a catastrophic event and the capacity to absorb, adapt, and rapidly recover from the event.

Resilience depends on robustness, resourcefulness, and recovery.

- Robustness is defined as "the ability to maintain critical operations and functions in the face of crisis" (DHS, 2009a). Robustness measures include barriers, cameras, alarms, access control, redundancy of critical infrastructure systems and components. Robustness measures also include mitigating construction techniques that are designed to prevent a structure from collapsing after an explosion, structural retrofits, and debris mitigation techniques such as window films.
- Resourcefulness is defined as "the ability to skillfully prepare for, respond to and manage a crisis or disruption as it unfolds" (DHS, 2009a). Resourcefulness factors include training and preparedness, exercises, information sharing, security awareness programs, and ongoing assessment of risk.
- Recovery is defined as "the ability to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption" (DHS, 2009a).

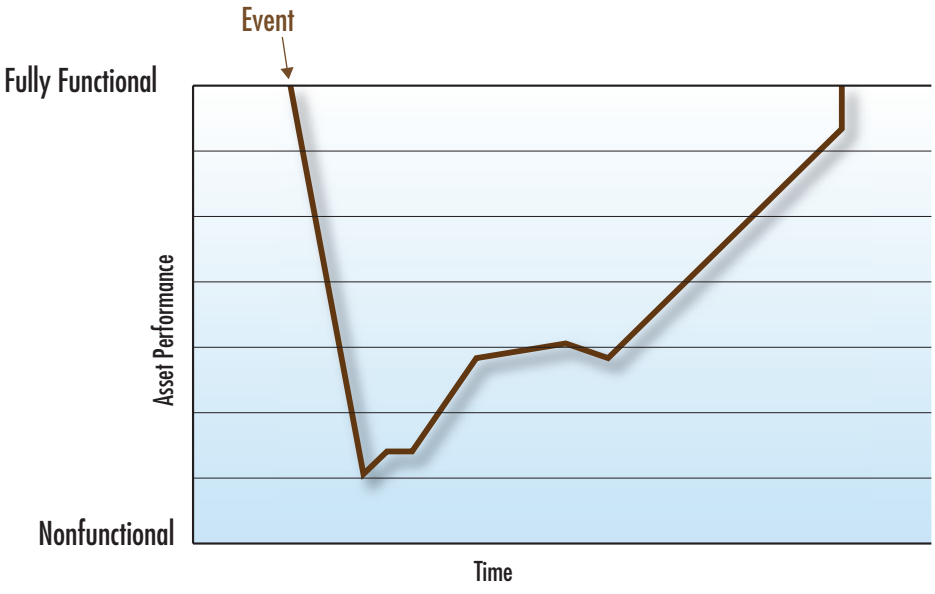


Figure 1-1:
Example of resilience

1.4 Organization of the Manual

The information in this manual is organized as follows:

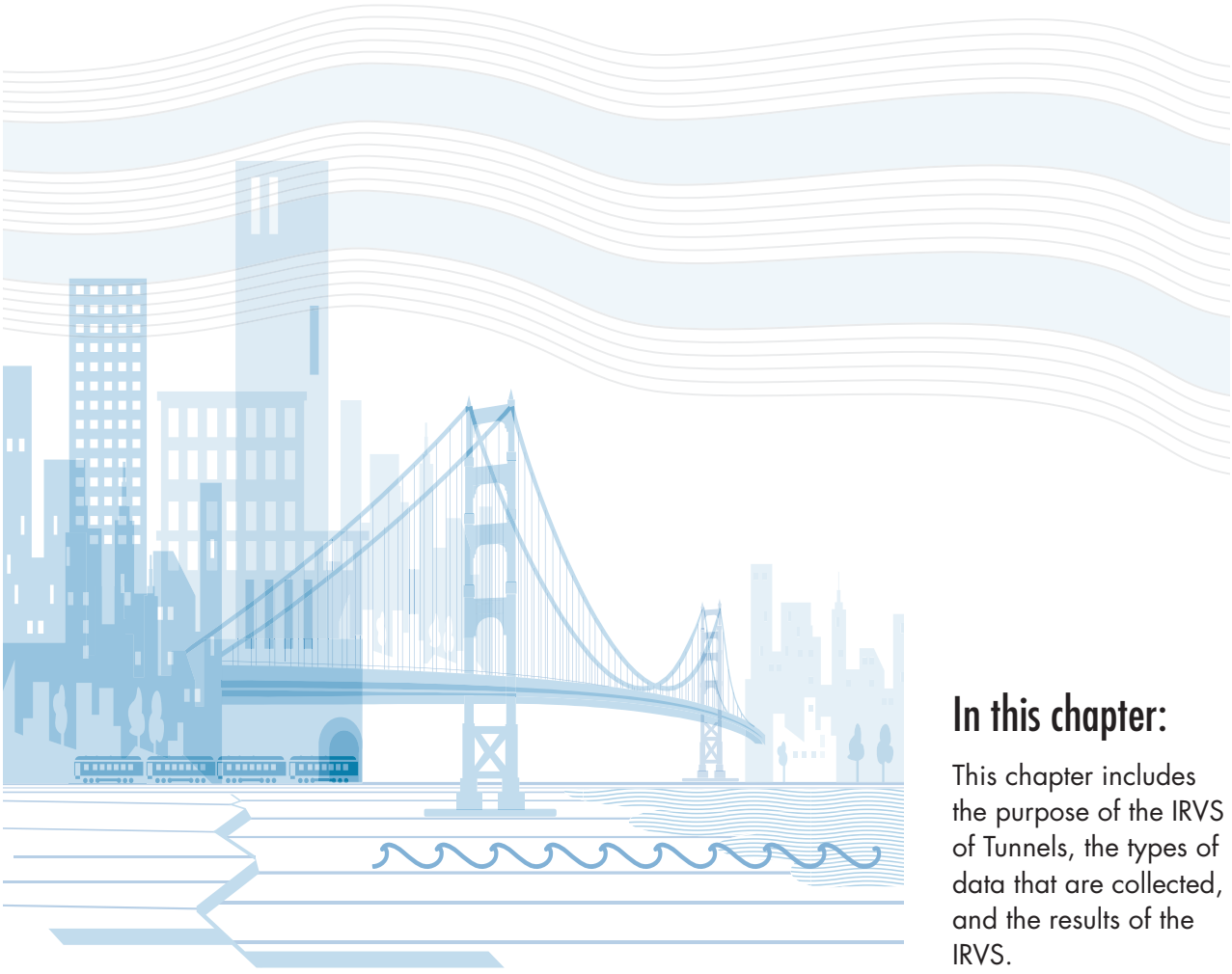
- Introduction to the IRVS of Tunnels (Chapter 2)
- Conducting an IRVS of Tunnels (Chapter 3)
- Completing the Data Collection Form (Chapter 4)
- References (Chapter 5)

Supplemental information is provided in the following appendices:

- Appendix A: Acronyms and Abbreviations
- Appendix B: Glossary
- Appendix C: IRVS Database User Guide
- Appendix D: Data Collection Form: Paper Version
- Appendix E: DHS Infrastructure Taxonomy

2

Introduction to IRVS of Tunnels



In this chapter:

This chapter includes the purpose of the IRVS of Tunnels, the types of data that are collected, and the results of the IRVS.

This chapter includes the purpose of the IRVS of Tunnels, the types of data that are collected, and the results of the IRVS. Chapters 3 and 4 explain how to conduct the IRVS input data into the IRVS Database, respectively.

2.1 Purpose of the IRVS of Tunnels

A tunnel is defined as a passageway through or under an obstruction such as a city, mountain, river, or harbor. A tunnel may be used for pedestrian traffic, vehicular road traffic, or rail traffic or as a canal. Tunnels are typically completely enclosed except for openings for egress, commonly at each end. Only tunnels used in transportation systems (mass transit and highway) are addressed in the IRVS of Tunnels methodology.

A tunnel is defined as a passageway through or under an obstruction such as a city, mountain, river, or harbor.

The purpose of the IRVS of Tunnels is to assess a tunnel's risk of a terrorist attack or selected natural disaster (fire or flooding) and the resiliency of the tunnel (the ability to recover from such an event). The results of the assessment can be used to avoid or minimize catastrophic losses—fatalities, injuries, tunnel destruction or damage, and business interruption— from a terrorist attack or natural disaster.

The purpose of the IRVS of Tunnels is to assess a tunnel's risk of a terrorist attack or selected natural disaster (fire or flooding) and the resiliency of the tunnel (the ability to recover from such an event).

The IRVS provides an assessment of the risk of a tunnel by evaluating the consequences of, threat of, and vulnerability to a terrorist attack or natural disaster. The IRVS also provides an assessment of the resilience of a tunnel by evaluating the tunnel's robustness, resourcefulness, and potential for recovery.

- The IRVS generates separate scores for risk and resilience. The information that is collected and the scores can be used to help:
- Identify, collect, and store vulnerability data that allow re-examination of risks during consideration of protective measures or after protective measures have been implemented
- Collect and store reported assessment information for tunnel management
- Prioritize vulnerabilities and consequences in a mass transit system indicating which tunnels may be more at risk and require more detailed analysis and/or higher protection

- Determine and report risks in a particular highway or mass transit tunnel in order to allocate potential resources to reduce major vulnerabilities cost effectively
- Understand potential cascading effects to the mass transit system by assessing a group of mass transit tunnels
- Understand resilience, potential down time, and economic and social implications if a tunnel is affected by a catastrophic event
- Identify which security measures should be implemented immediately during high alerts
- Anticipate the increased risks during special events that affect the peak flows of the tunnel in order to plan properly and implement protective measures; special events are events that cause an abnormally high volume of ridership (e.g., sporting events, concerts, festivals)

The **risk score** is a numeric value that describes the risk of catastrophic loss from a terrorist attack or natural disaster at a mass transit station.

The **resilience score** is a numeric value that describes the ability of a mass transit station to resist, absorb, and recover from a potentially disruptive event at a mass transit station.

2.2 Stakeholders

The stakeholder is the group or entity that decides to conduct an IRVS, owns the results of the IRVS, and makes many of the decisions regarding the IRVS. In most cases, the stakeholder is the owner or operating authority of the tunnel or group of tunnels but can also be a law enforcement agency or a Federal, State, or local government agency.

The stakeholder or stakeholder's personnel may conduct the IRVS. For example, a mass transit authority may create a task group consisting of its security personnel and engineers to conduct an IRVS of the mass transit system. The mass transit system may opt to hire a consulting group to conduct the IRVS.

2.3 Screeners

The IRVS was developed so that screeners can be local operators, law enforcement, and others without an engineering or architectural background can conduct an IRVS with a reasonable level of certainty after brief training, thus reserving technical experts such as engineers and architects for more in-depth assessments. See Section 3.3 for more information about screeners and the IRVS team.

2.4 Time Required for the IRVS

One of the strengths of the IRVS of Tunnels is how quickly it can be completed. An assessment can typically be conducted in approximately 2 days by one or two screeners, facility management, and key staff. The field assessment is designed to be completed by two screeners in a few, depending on the complexity of the tunnel and the availability of information prior to the assessment.

2.5 Characteristics, Attributes, and Data

This section describes the types of data that are collected during the IRVS and how the data are recorded and stored.

The various characteristics of tunnels are evaluated in the IRVS. A characteristic is a physical component, function, or operation that relates to consequences, threat, and vulnerability. Examples of characteristics are the number of tracks/lanes, number of entrances, natural protective barriers, presence of hazardous materials, construction material, and tunnel medium.

"**Characteristic**" refers to the physical components, function, and operation of a mass transit station. "**Attribute**" is a subcategory of a characteristic.

An attribute is a subcategory of a characteristic. For example, for tunnel medium (characteristic), the attribute may be below grade (above water table), below grade (below water table), or under water. Screeners select one attribute from a set of attribute options for each characteristic. Some characteristics have multiple sets of attributes, which reflect the need to normalize regional and other types of disparities.

Attributes are weighted depending on their degree of risk. For example, an underwater tunnel has the most risk compared to other elevations and is therefore given the heaviest weight of the attribute options for elevation.

Characteristics are grouped into the risk components of consequences, threat, and vulnerability, depending on which component the characteristic would affect. See Section 2.5.2 for information on the components of risk. Some characteristics affect more than one component.

The attributes of characteristics that are more important than others are weighted more heavily than the attributes of less important characteristics. Characteristics with heavily weighted attributes require careful evaluation because of their influence on the risk score. A small difference in the assessment of these characteristics can change the risk and resilience scores significantly.

2.5.1 Consequences, Threat, and Vulnerability

As noted in Section 2.5.1, characteristics are grouped into the components of risk—consequences, threat, and vulnerability.

Consequence is the effect of an event, incident, or occurrence and reflects the level, duration, and nature of the loss resulting from the incident.

- As defined in the NIPP (DHS, 2009), consequence is the effect of an event, incident, or occurrence and reflects the level, duration, and nature of the loss resulting from the incident. Consequences are divided into four categories: public health and safety, economic, psychological, and governance/mission impacts.
  - The category of **public health and safety** reflects the effect on human life and physical well-being (e.g., fatalities, injuries/illness). **Economic loss** includes direct loss (e.g., cost to rebuild an asset, cost to respond to and recover from the event) and indirect loss (e.g., costs resulting from the disruption of a product or service, long-term costs from environmental damage). The **psychological effect** refers to the effect on public morale, which includes the possible changes in the public's sense of safety and well-being after a significant event and possible subsequent aberrant behavior. The **governance/mission effect** is the effect on government's or industry's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

Consequences are divided into four categories: public health and safety, economic, psychological, and governance/mission impacts.

  - The consequences that are considered in the IRVS are based on the criteria set forth in Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection. HSPD-7 establishes a framework to identify, prioritize, and protect CIKR from terrorist attacks and natural hazards, with an emphasis on protecting against catastrophic health effects and mass casualties.
- **Threat** is defined as a natural or manmade occurrence that harms or indicates the potential to harm life, information, operations, the environment, and/or property.
- **Vulnerability** is defined as a physical feature or operational attribute that renders a station open to exploitation or susceptible to a give hazard. Vulnerabilities may be associated with physical, cyber, or human factors. The assessment of vulnerabilities involves evaluation of specific threats to the asset to identify areas of weakness that could result in consequences of concern.

2.5.2 Subjective Judgments

Screeners may use subjective judgment when selecting attributes. The information in the catalog is intended in part to minimize the number of times the screener must use subjective judgment.

2.5.3 IRVS Catalog

The IRVS catalog contains the characteristics and associated attributes that are evaluated during the IRVS and information about the characteristics and attributes to help the screener. Characteristics are divided into consequences, threat, and vulnerability.

The catalog is essential in an IRVS assessment. The catalog is provided in Chapter 4 of this manual and also digitally in the IRVS database. See Section 2.5.5 for information about the IRVS database.

2.5.4 Electronic Data Collection Form

In the IRVS assessment, the screener records data using the electronic Data Collection Form (DCF) in the IRVS Database (see Section 2.5.5). The screener may opt to use a paper version of the DCF, but the paper version is not recommended because the data have to be transferred to the electronic version later, which takes times and creates the potential for errors. The screener can input data into the electronic DCF using a laptop or tablet computer. The paper version is provided in Appendix D.

The first page of the DCF contains general tunnel information and target density information (i.e., the number of high-value targets near the tunnel). The subsequent pages of the DCF contain characteristics and attribute options for consequences, threat, and vulnerability. The attribute options are listed in order of least degree of risk to highest degree of risk.

See Chapter 4 for information on completing the DCF.

2.5.5 IRVS Database

The IRVS database is a user-friendly data collection and management tool that includes the IRVS catalog and the DCF. The database is a standalone application that runs on computers with MS Access. Reports are generated as text files or files that can be imported into MS Word or MS Excel for editing and formatting.

2.5.5.1 Database Synchronization

The database can be accessed by multiple computers simultaneously. For example, screeners use the DCF in the database to record data in

the field, and a computer at an organization's headquarters analyzes the data and prints reports. The database is kept up-to-date using the import/export feature (see Appendix C) and by synchronizing the database through the authority's secure network.

2.5.5.2 Use of the Database by Tunnel Managers

The IRVS database can be used to facilitate the management of tunnel. Tunnel managers can use vulnerability and risk data when considering the implementation of protective measures. During periods of high alert, the database can be used to identify which security measures should be put in place immediately.

2.5.6 Links

Some characteristics affect more than one risk component. For example, the number of riders affects both consequences and threat. As the number of riders increases, the consequences and threat ratings are both expected to increase. The number of riders is therefore linked to two risk components and has a similar effect on both components.

Some characteristics affect more than one risk component.

Some linked characteristics have different effects on risk components. For example, an underwater tunnel would increase flooding vulnerability while reducing the vulnerability to external attacks.

2.6 IRVS Risk and Resilience Scores

The IRVS generates scores for risk and resilience.

2.6.1 Risk Score

The risk score is based on the consequences, threat, and vulnerability ratings for each of the 10 threat scenarios. Consequences, threat, and vulnerability ratings are explained in Section 2.6.1.1, and threat scenarios are explained in Section 2.6.1.2.

2.6.1.1 Consequence, Threat, and Vulnerability Ratings

The IRVS generates ratings for consequences, threat, and vulnerability.

- A **consequences rating** represents the degree of debilitation that would result from the incapacitation or destruction of an asset after a catastrophic event that causes injuries or fatalities, social and economic losses, and/or business interruption. Consequences are rated from the perspective of a tunnel's stakeholders, not terrorists.

- The t**hreat rating** represents the likelihood that a tunnel will be affected by a terrorist attack or natural disaster (fire or flooding) and that the losses will be catastrophic (fatalities, injuries, damage, or business interruption).
- The **vulnerability rating** is defined as the likelihood of damage and loss at a tunnel as a result of a terrorist attack and natural hazard (fire, flood).

  The vulnerability rating is the most important and in-depth part of the IRVS. Unlike consequences and threats, vulnerabilities can be controlled or mitigated by the stakeholder. The vulnerability rating is crucial for determining protective measures and corrective actions that can be designed or implemented to reduce the identified vulnerabilities.

2.6.1.2 Threat Types and Scenarios

In the IRVS, risk is assessed with respect to a threat scenario or set of scenarios. The IRVS includes an assessment of the risk of both terrorist attacks and selected natural hazards. Risks are divided into four categories: (1) blast, (2) chemical, biological, or radiological (CBR) attack, (3) fire, and (4) other. Each category is subdivided into threat scenarios (see Table 2 1). The scenarios represent the location of the source of harm. All components of risk (i.e., consequences, threat, and vulnerability) are evaluated for each scenario.

Table 2-1: Threat Types and Threat Scenarios

Threat Type	Threat Scenario
Blast	Internal External (direct) External (collateral)
CBR	Internal (platforms/plaza/etc.) Internal (tunnel) External
Fire	Internal External Tunnel/Track/Smoke
Other	Flood Collision (grade/tunnel/elevated) Cyber

CBR = chemical, biological, or radiological

- **Blast**
  - **Internal –** Intrusion into the tunnel by a person or persons with the intent to attack the tunnel with an explosive device.
  - **External (direct) –** Use of an explosive device to attack the tunnel from the exterior. The tunnel is the primary target.
  - **External (collateral) –** An attack with explosive devices on a target within a 300-foot radius of the tunnel (e.g., a bomb explosion in a plaza adjacent to a tunnel). The tunnel is not the primary target but is susceptible to collateral damage. The severity depends on the proximity to the target and the magnitude of the threat.
- **Chemical, biological, or radiological (CBR) release**
  - **Internal –** Ground release of an airborne CBR agent inside the tunnel.
  - **External –** The ground release of an airborne chemical, biological, or radiological agent from the exterior of the tunnel.
- **Fire**
  - **Internal –**A fire outside the tunnel entrances that threatens the operations of the tunnel itself. An example would be a tunnel entrance next to or under a building that is on fire, thus threatening the operations and structure of the tunnel.
  - **Tunnel/Track/Smoke –** The spread of fire inside the operating areas servicing vehicles/trains of the tunnel. This includes smoke from the tracks of trains using the tunnel.
- **Other**
  - **Flood –** The tube of the tunnel being submerged in water threatening the operations and users inside the tunnel.
  - **Collision –** A vehicular impact to the tunnel causing damage to the structure and threatening operations.
  - **Cyber –** An attack on the tunnel through any combination of facilities, equipment, personnel, procedures, and communications integrated through cyber networks or control systems.

2.6.1.3 Calculation of the Risk Score

The risk scoring procedure used in the IRVS is based on the risk assessment equation in P-426, *Reference Manual to Mitigate Potential Terrorist Attack Against Buildings* (DHS, 2011c) and the NIPP framework assessing risks (DHS, 2009b).

The procedure is as follows:

1. The consequences, threat, and vulnerability ratings are generated for each threat scenario.
2. The consequences, threat, and vulnerability ratings for each scenario are combined using the following equation to produce a risk score for the scenario (de-aggregated risk score).

Equation

$$Risk = C \times T \times V \quad (1)$$

where

***C* = Consequences Rating** – degree of debilitation that would be caused by the incapacity or destruction of an asset. The consequences rating includes both monetary value and the value to a system or community.

***T* = Threat Rating** – any indication, circumstance, or event with the potential to cause loss of, or damage to, an asset.

***V* = Vulnerability Rating** – any weakness that can be exploited by an aggressor to make an asset susceptible to damage.

The de-aggregated risk score for each scenario ranges from 0.01 to 10. De-aggregated risk scores are color-coded as low (green), moderate (yellow), and high risk (red) in the IRVS database.

The de-aggregated risk score for each threat scenario provides more information about a station's risk to a specific threat than the overall risk (aggregated) score.

3. The 12 de-aggregated risk scores are combined using the statistical algorithm shown below to produce a single overall risk score (aggregated risk score) for the station.

Equation

$$R = \propto \sqrt[n1]{\sum_{i=1}^{n2} R_i^{n1}} \quad (2)$$

and

Equation

$$R_i = \sqrt[3]{C_i \times T_i \times V_i} \quad (3)$$

where

$\propto$ = scaling factor of 1/12

R = aggregated (overall) risk

$n2$ = 12 (total number of threat scenarios)

$n1$ = 10 (power value)

R_i = risk score of the i^{th} threat scenario

C_i = consequences rating of the ith threat scenario

T_i = threat rating of the ith threat scenario

V_i = vulnerability rating of the ith threat scenario

C_i, T_i, and V_i are all scaled to be in the range of 0.01 to 10. As such, the resulting risk score for the i^{th} threat scenario is also in the range of 0.01 to 10. The overall risk score (aggregated) is displayed as a percentage to indicate the level of risk associated with the tunnel.

The risk score are color-coded as low (green), moderate (yellow), and high risk (red) in the IRVS database. Table 2-2 indicates the different levels of risk.

Table 2-2: Risk Levels

Risk Level	Risk Score
High	>66%
Moderate	≥33%, ≤66%
Low	<33%

2.6.2 Resilience Score

The characteristics in the IRVS cover most of the important issues that affect the resilience of a tunnel. Each characteristic can affect the quality of performance (robustness), resourcefulness, and/or time and speed of recovery. Each attribute option for the characteristics that pertain to resilience is assigned a weight ranging from 0 to 10. The weight represents the importance of the attribute in the resiliency of the tunnel. At the end of the assessment, all of the adjusted weights of the attributes that control quality of performance, Q_j , are summed. The quality of performance describes the ability of the tunnel to maintain critical operations and function. Similarly, all of the adjusted weights of the characteristics that control recovery and resourcefulness, also known as the time measure, T_i, are summed. The time measure describes preparedness efforts (such as training, plans, and policies) and the ability to re-institute operations after a hazard event. The sum of Q_j and T_i are inserted into the following equations:

Equation

$$Q_{TOTAL} = 10\left(\frac{\sum_{i=1}^{N} Q_i}{\sum_{i=1}^{N} Q_i|_{MAX}}\right) \quad (4)$$

and

Equation

$$T_{TOTAL} = 10\left(\frac{\sum_{i=1}^{N} T_i}{\sum_{i=1}^{N} T_i|_{MAX}}\right) \quad (5)$$

where

Q_{TOTAL} = scaled quality of performance

T_{TOTAL} = scaled time measure

Q_i = quality of performance (robustness)

N = upper boundary (number of characteristics with a weight being summed)

T_i = time measure (recovery and resourcefulness)

$Q_{i|MAX}$ = maximum quality of performance

$T_{i|MAX}$ = maximum time measure

$Q_{i|MAX}$ and $T_{i|MAX}$ represent the maximum weighted values of the quality of performance and the recovery/robustness values, respectively. Now the values of Q_{TOTAL} and T_{TOTAL} represent a scaled, accurate measure of quality of performance and time measure that control resiliency (the two axes in Figure 1-1). The scale for both variables ranges from 0.01 to 10. The objective value of the tunnel resilience is

Equation

$$\textbf{\textit{RES = 100 – }}(Q_{TOTAL}\ T_{TOTAL}) \quad (6)$$

where

RES = *resilience*

Thus, a *RES* of 0% indicates there is no resilience in the tunnel when affected by the postulated hazard. A *RES* of 100% indicates a perfect resilience in the tunnel when affected by the postulated hazard.

Resilience scores can be used in decision-making and planning for hazardous events for the asset (tunnel). These scores can also be used in planning for community (network) resiliency. Table 2-3 indicates the levels of resilience and how to interpret these levels.

Table 2-3: Resilience Levels

Resilience Level	Resilience Score	Description
High	>66%	The tunnel has taken reasonable steps to maintain continuity of operations and/or has taken reasonable action to ensure that key functions will not be significantly affected by an event.
Medium	≥33%, ≤66%	The tunnel has taken moderate steps to maintain continuity of operations and/or has taken moderate action to ensure that key functions will not be significantly affected by an event.
Low	<33%	The tunnel has taken few or no steps to maintain continuity of operations and/or has taken little or no action to ensure that key functions will not be significantly affected by an event.

2.7 Other Considerations

2.7.1 Assessing Vehicular Tunnels

Vehicular tunnels are typically shorter than rail tunnels and the conditions surrounding the tunnel typically do not change significantly from portal to portal.

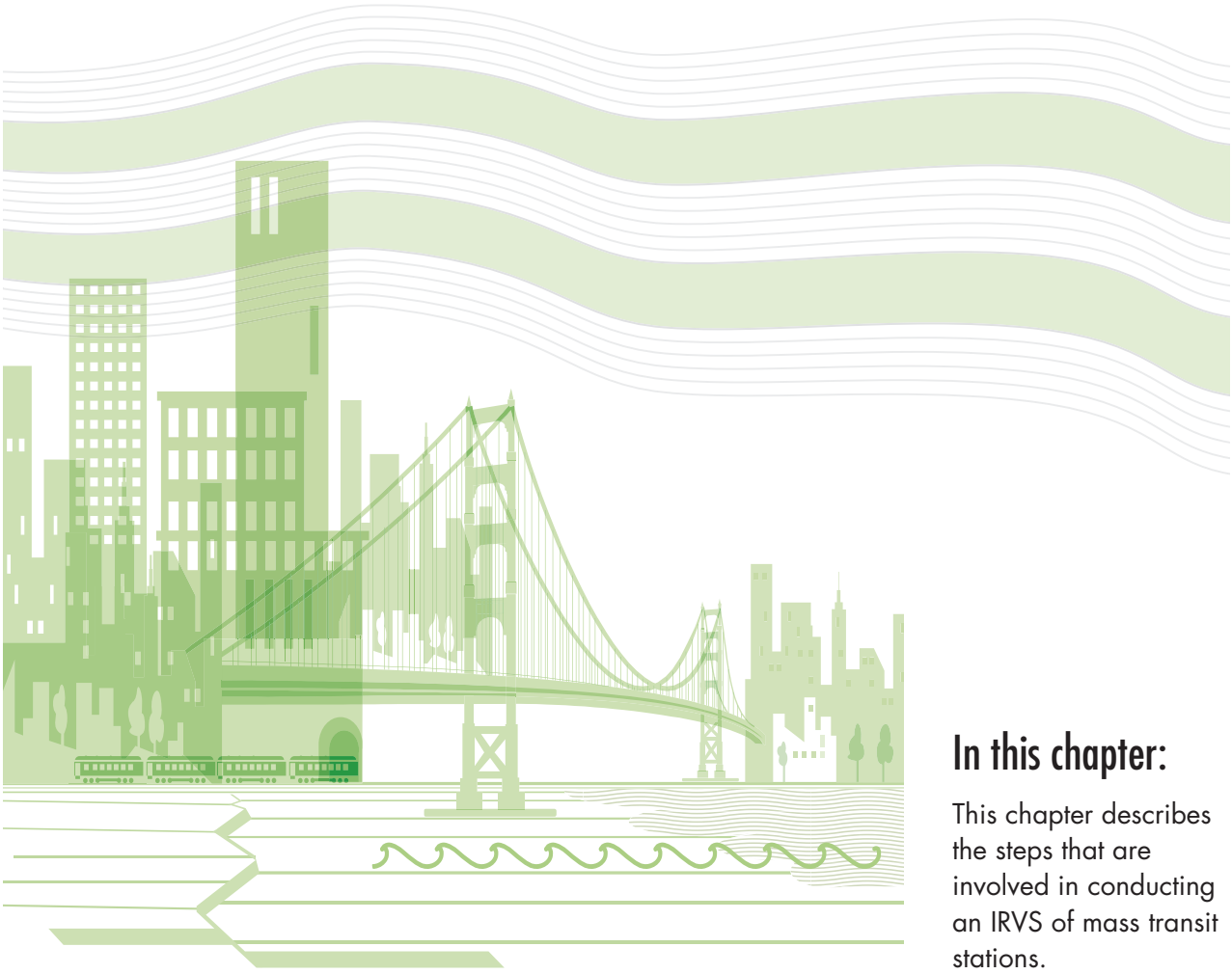
2.7.2 Assessing Rail Tunnels

Depending on the system and city, rail tunnels can span long distances and have many variations in the sections of the tunnel. For example, one section may be under a dense urban area while another section may be underwater. In addition, rail tunnels can have several stations between the tunnel portals. To account for the variations, the screener should:

- Assess rail tunnels in sections
- Assess rail tunnels at the most vulnerable location (e.g., where the tunnel passes under a major downtown area of a city)

3

Conducting an IRVS of Tunnels



In this chapter:

This chapter describes the steps that are involved in conducting an IRVS of mass transit stations.

This chapter describes the steps that are involved in conducting an IRVS of tunnels (see Table 3-1). The IRVS process can be adjusted as needed.

Chapter 4 describes how to complete the Data Collection Form (DCF).

Table 3-1: Steps in the IRVS of Mass Transit Stations

Pre-Field Activities	• Select the tunnels to be assessed • Identify the IRVS team • Train the IRVS team • Identify key objectives of the IRVS • Complete as much of the DCF as possible by reviewing publicly available information and available materials from transit authorities, including operations and security procedures, policies, and construction drawings • Identify the conditions for the field assessment • Set up a meeting with key staff and schedule the tunnel tour • Assemble the equipment that is needed for the field assessment
Field Assessment	• Interview and meet with key staff and stakeholders • Tour the exterior and publicly accessible areas of the tunnel • Tour the critical areas of the interior of the tunnel • Record data on the DCF
Post-Field Activities	• Transfer data from the paper version of the DCF to the electronic DCF if necessary • Use the scores in a variety of ways including identifying the tunnels that require a more detailed assessment • Summarize the results in a written report

3.1 Pre-Field Activities

The accuracy of the IRVS will be improved if the screeners obtain and review relevant information about the tunnel prior to the field assessment and also review the IRVS methodology. A review of the IRVS methodology by the team of screeners for a group of tunnels prior to the assessments will help ensure consistency among assessments, a high quality of collected data, and uniformity of decisions among screeners.

3.1.1 Selecting Tunnels To Be Assessed

The IRVS can be used to assess a single tunnel or a group of tunnels in a highway or mass transit system or region. The stakeholder typically selects the tunnels that will be assessed (see Section 2.2 for more information on the stakeholder). Budget is often a factor in the selection of tunnels for the IRVS.

3.1.2 Identifying the IRVS Team

The stakeholder or designee appoints the IRVS team leader who is responsible for identifying the IRVS team. The team leader should be familiar with risk assessment and transportation systems. The IRVS team should include members who are knowledgeable about tunnel systems and security concepts and should include at least one individual familiar with structural engineering or construction and operations of a tunnel.

The IRVS was developed so that screeners inside or outside the design community could conduct an IRVS with a reasonable level of certainty after brief training, thus reserving technical experts such as engineers and architects for more in-depth assessments. The more knowledgeable the screeners, the more accurate the assessment and, potentially, the more accurate the results. Training is recommended to ensure that the IRVS team understands the IRVS concepts. At a minimum, the IRVS team should review this manual.

3.1.3 Training the IRVS Team

Training should be required to ensure accuracy and uniformity of decisions among screeners. Training includes reviewing the IRVS methodology. The review should include:

- Tunnel systems (e.g., site design; architectural, mechanical, electrical, plumbing, fire protection, security, and cyber systems)
- How to complete the DCF (see Chapter 4)
- How to use IRVS database (see Section 2.5.6)
- What screeners should bring to the field assessment (see Section 3.1.9)
- What screeners should look for when performing the field assessment (See Section 3.2.2)
- How to account for uncertainty (see Section 4.2)

The training should also include a desktop exercise, which is a simulated IRVS conducted in a classroom using photographs of tunnels. The desktop exercise can be created by gathering photographs of and information about an actual tunnel.

3.1.4 Identifying the IRVS Objectives

The stakeholders and IRVS team should determine the objectives of the assessment early in the pre-field activities. Examples of objectives are:

- Assessment of a group of tunnels to determine which tunnels require more detailed analysis
- Evaluation of the risk for a tunnel during a period of high threat alert in order to implement protective measures
- Prioritization of a group of tunnels for mitigation
- Preparation of a risk report of tunnels in a system in order to apply for grant funding

Objectives define outcomes and conditions of the assessment. For instance, if the objective is to evaluate the risk of a tunnel during a period of high threat alert, the condition for the assessment will be worst case and the outcome will be to establish immediate protective measures to lower the risk score. Objectives can also help determine the resources, time, and effort that are needed and how the risk and resiliency results will be used. If the objective includes assessing a group of tunnels, more time and effort will be needed than when only a single tunnel is assessed. Objectives may vary across and within transportation systems.

The goal of the IRVS is to enhance protection and resiliency through the implementation of focused risk-reduction strategies.

The goal of the IRVS is to enhance protection and resiliency through the implementation of focused risk-reduction strategies.

3.1.5 Evaluating Target Zones and Density

Two considerations when selecting a tunnel for IRVS are the proximity of the tunnel to other critical facilities and the presence of other high-profile targets near the tunnel. Proximity of targets creates two possible scenarios of concern. In the first scenario, the tunnel itself is the target, and collateral damage to nearby critical facilities will increase damage and the severity of the attack. In the other scenario, the tunnel is not the target, but there are high-profile targets near the tunnel, and the tunnel is subjected to collateral damage that varies in

severity depending on the hardiness of the structure, proximity to the target, and magnitude of the threat. In the IRVS, the concept of target density is part of the consequences, threat, and vulnerability ratings. The IRVS of tunnels is designed to address both target and non-target tunnels.

The IRVS of mass transit stations is designed to address both target and non-target tunnels.

In the IRVS, the following target zones are considered (see Figure 3-1):

- Zone 1 refers to an attack occurring less than 300 feet from the subject tunnel.
- Zone 2 refers to an attack occurring at least 300 feet but not more than 1,000 feet from the tunnel.

Information regarding the target density is collected on the first page of the DCF (see Section 4.2). The target density can be calculated using open source information such as Google maps or Bing maps. In addition, the IRVS database includes an application for plotting the target density rings in Google Earth (requires installation on a computer) using the coordinates of the tunnel. The target density is calculated using the 18 CIKR Sectors that are identified in HSPD-7.

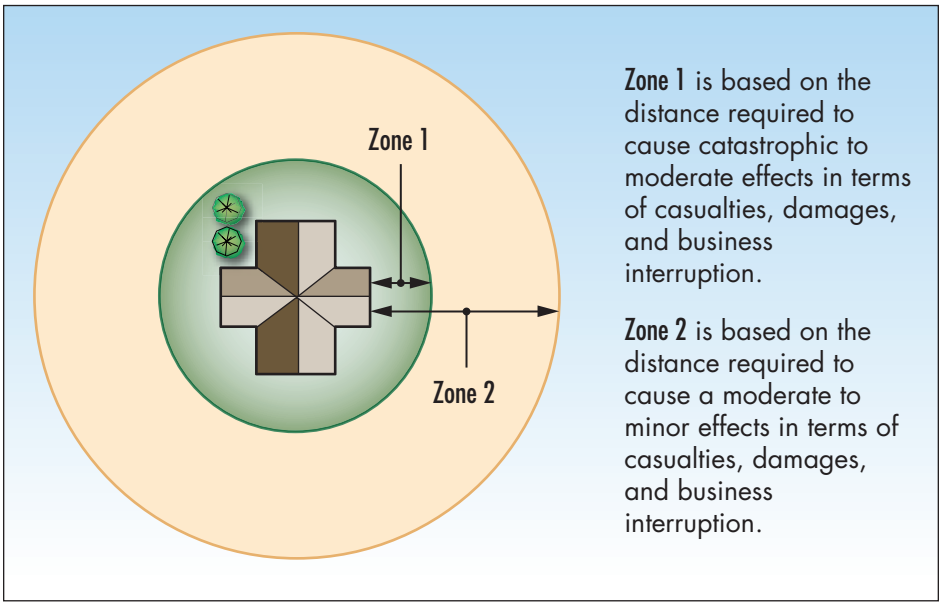


Figure 3-1:
Target Zones 1 and 2

3.1.6 Gathering Pre-Field Data

The IRVS team should complete as much of the DCF as possible before the field assessment by reviewing publicly available information and information that is provided by the transit agency (e.g., operations and security procedures, policies, construction drawings). Electronic documents can be stored in the IRVS database as MS Word files or PDFs. Documents that are not available electronically can be scanned and imported into the database.

Examples of documents that can be useful are:

- Drawings for original design and any implemented modifications
- Prior vulnerability assessment data
- Emergency response and disaster recovery plans
- Security master plan
- Hazardous materials plans
- Site plans of utility and communications system
- Historical reports regarding the tunnel
- Facility systems operational capability
- Reports of incident in the tunnel (e.g., misconduct)

The IRVS team should also review emergency plans, policies, and procedures. These documents are useful in evaluating characteristics related to resilience. Examples of such documents are:

- Emergency notification procedures
- Emergency evacuation procedures
- First responder access and routing
- Shelter-in-place procedures
- Exercise of plans

The screener can also obtain information by conducting phone interviews of transportation system authorities, stakeholders, and key tunnel staff.

3.1.7 Identifying Conditions for the Field Assessment

IRVS results can be affected by the timing of the field assessment. For example, a mass transit tunnel may have low ridership during the work week

but high ridership during a special weekend event at a nearby venue (e.g., sporting event, concert, festival). Ridership is relevant to all three risk components (consequences, threat, and vulnerability).

To avoid variations that can distort the scores, the IRVS team and stakeholders should determine before the field assessment which conditions will be considered.

To avoid variations that can distort the scores, the IRVS team and stakeholders should determine before the field assessment which conditions will be considered. The two conditions are:

- **Current "as-seen" conditions:** The tunnel is assessed for the situation and conditions present at the time of the screening.
- **Worst-case or special event conditions:** The combination of conditions that would make the most harmful results.

Physical conditions should be considered at their most disadvantageous state. Reasonable worst-case conditions are recommended when assessing the risk of a terrorist attack because intelligent adversaries can choose circumstances in which targets are vulnerable and consequences maximized (NIPP, 2009). The concept of worst case should be moderated by reason, however; scenarios should not include numerous unlikely conditions unless the focus of the contingency and other types of planning is on rare or special events. On the other hand, scenarios should not be based simply on average conditions. Each type of tunnel has different characteristics that need to be assessed to accurately describe reasonable worst-case conditions. The IRVS team and stakeholders should establish the conditions that will be considered.

3.1.8 Scheduling a Meeting with Key Staff and Stakeholders and Scheduling the Tunnel Tour

The IRVS team should try to arrange a meeting or interview with key staff and stakeholders before or during the field assessment to review the information that was obtained before the field assessment. The IRVS team leader decides which key staff and stakeholders should be interviewed based on the composition of the team and the familiarity of the tunnel or transportation system. The team should prepare a list of questions before the meeting. Key personnel include:

- Chief of engineering
- Chief of security
- Chief of Information Technology
- Emergency manager

The IRVS team also needs to schedule the tunnel tour. The IRVS team should plan which areas of the tunnel (see Section 3.2.2) need to be viewed and obtain the proper permissions to survey the tunnel.

3.1.9 Assembling the Equipment for the Field Assessment

The screener should take the following to the field assessment:

- A laptop or tablet loaded with the IRVS database, which contains the DCF and catalog. The database user guide is included in this manual as Appendix C.
- The paper version of the DCF if a laptop or tablet is not available. The paper version is included in this manual as Appendix D.
- A digital camera for photographing the tunnel.

3.2 Field Assessment

The field assessment is an onsite visit to the tunnel whose purpose is to record and/or verify information on the DCF. Interviews with key tunnel personnel and stakeholders may be conducted during the field assessment. The visit involves observing exterior and interior areas of the tunnel.

3.2.1 Key Personnel and Stakeholder

The field assessment is an onsite visit to the tunnel to record and/or verify information that has already been recorded on the DCF. The visit includes interviewing key personnel and stakeholders and touring the tunnel.

3.2.2 Touring the Tunnel

The IRVS team should tour the exterior of the tunnel; publicly accessible areas; and internal, secure areas of the tunnel. The locations the screener should tour, if applicable, are:

- **Tunnel exterior**
  - Perimeter of tunnel and area above the tunnel (public areas and infrastructure above)
  - Approaches
  - All points of entry/egress
  - Ventilation structures (if applicable)
  - Connection stations (if applicable)
  - Waterside (if applicable)

- **Tunnel interior**
  - Tracks or lanes
  - Mechanical electrical and plumbing rooms
  - Emergency exits
  - Security rooms
  - Pump rooms or floodgates (if applicable)
  - Ventilation equipment (if applicable)

3.3 Post-Field Activities

The following activities are typically conducted after completing the DCF and the field assessment.

3.3.1 Transferring Data to the DCF

If the paper version of the DCF is used, the information must be transferred to the IRVS database in order to generate the risk and resiliency scores. Any photographs taken during the field assessment should be imported into the database.

3.3.2 Using the IRVS Scores

The IRVS of Tunnels is a quick and simple tool for obtaining a preliminary risk and resilience assessment. IRVS results can be used to:

- Identify the tunnels that require a more detailedassessment
- Prioritize tunnels for further evaluation
- Develop emergency preparedness plans for high-threat alerts
- Plan post-event evacuation, rescue, recovery, and safety evaluation efforts
- Prioritize mitigation needs
- Conduct a "what if" exercise by selecting different attributes to see how the scores are affected.
- Compare the scores of various threat scenarios to identify the relative exposure of the tunnels to different threats. Risk scores for different scenarios can be compared.
- Develop tunnel-specific vulnerability information

The IRVS of Tunnels is a quick and simple tool for obtaining a preliminary risk and resilience assessment.

3.3.3 Identifying Tunnels that Require Further Analysis

Depending on the objectives of the IRVS assessment, the IRVS team and stakeholders may identify tunnels requiring further analysis (a more detailed assessment). The IRVS team and stakeholders must determine the level of risk and resiliency that is considered unacceptable and would therefore trigger a more detailed assessment recommendation. Unacceptable risk and resilience may be defined differently for different tunnel systems based on the conditions of the system (e.g., size, locality, number of riders, performance objectives).

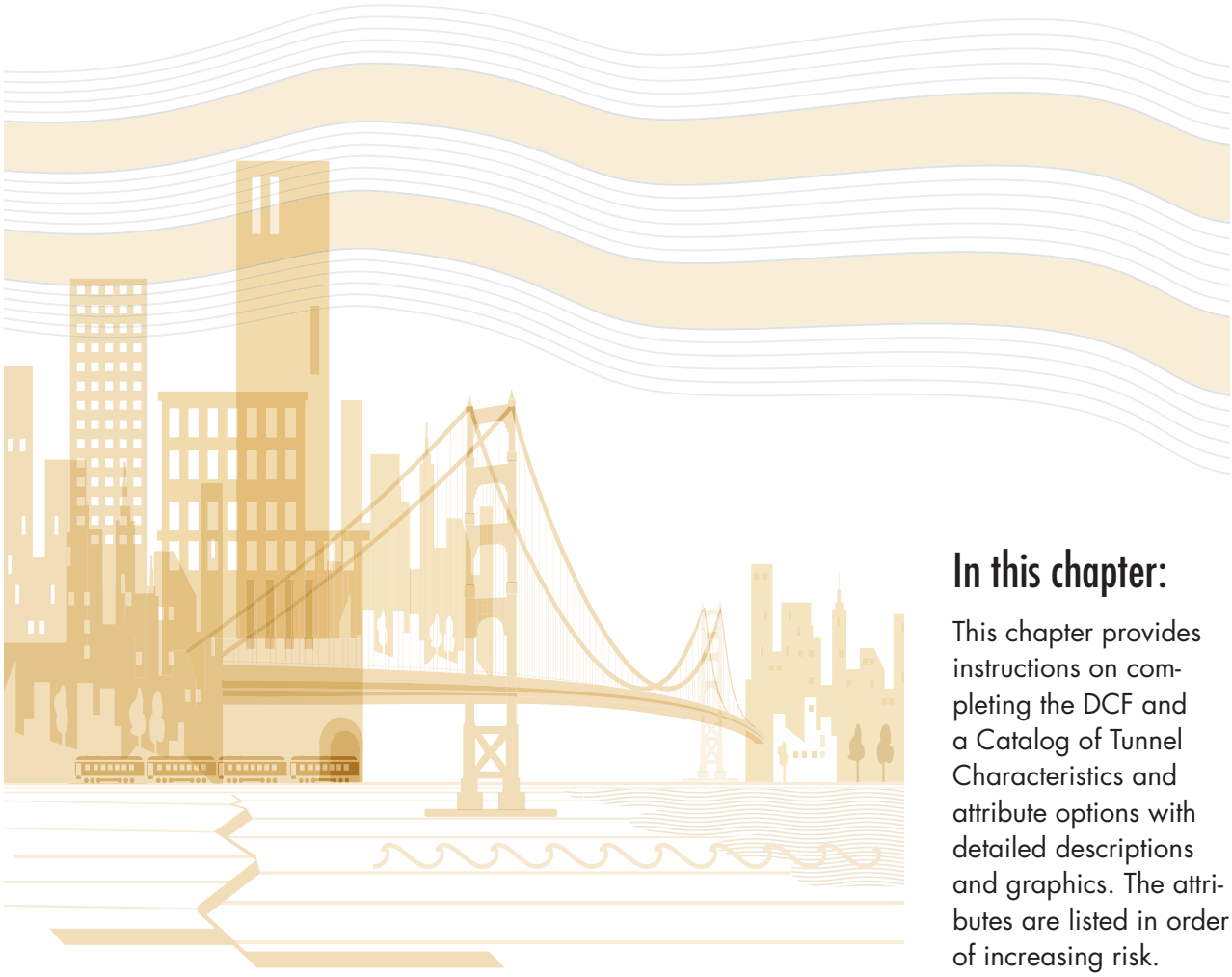
Generally, the risk and resilience can be interpreted as unacceptable when the risk score is above 70% and the resilience score is below 30%.

3.3.4 Preparing a Written Report

The IRVS database can be used to generate a generic report for one tunnel or a group of tunnels. The report includes the information that was input into the database and the risk and resiliency scores. The report is generated as an MS Word document and can be edited by the IRVS team.

4

Completing the Data Collection Form



In this chapter:

This chapter provides instructions on completing the DCF and a Catalog of Tunnel Characteristics and attribute options with detailed descriptions and graphics. The attributes are listed in order of increasing risk.

Information that is collected during the IRVS is recorded electronically on the Data Collection Form (DCF) or on paper using the paper version of the DCF. The screener can input data into the DCF using a laptop or tablet computer. If the paper version is used, the information has to be transferred to the electronic version, so using the electronic version is more efficient. The paper version is provided in Appendix D.

This chapter provides instructions on completing the DCF and a catalog of tunnel characteristics and attribute options with detailed descriptions and graphics. The attributes are listed in order of increasing risk.

The DCF is typically completed during the field assessment, but it can also be completed before or after the field assessment.

- **Before the field assessment –** The DCF is completed collectively by the IRVS team and key personnel during a desktop workshop, and the information is verified during the field assessment. Completing the DCF before the field assessment is typically done by screeners who are familiar with the tunnel or when the available information makes it possible.
- **During the field assessment –** The DCF is completed during the field assessment either electronically or using the paper version.
- **After the field assessment –** The IRVS team records observations, conducts interviews, and takes pictures during the field assessment. After returning from the field assessment, the IRVS team collectively completes the DCF.

The DCF should be completed according to the tunnel conditions that have been selected (see Section 3.1.6). Screeners should document the assessment as completely as possible to optimize the accuracy of the risk and resiliency scores.

4.1 Accounting for Uncertainty

The accuracy of the risk and resiliency scores rely on an accurate and thorough completion of the DCF. All characteristics must be evaluated before risk and resiliency scores can be calculated. If a screener is unsure which attribute is correct for a particular characteristic, the screener should document observations using the comments tab and should do one of the following:

The accuracy of the risk and resiliency scores rely on an accurate and thorough completion of the DCF.

- Select “Not Applicable” when available

- Make an educated guess based on professional or engineering judgment
- Select the attribute that is most common in other similar tunnels in the system

Where two or more attributes for one characteristic could be selected, the screener should select the dominant attribute . When one attribute is not clearly dominant and an educated guess is not possible because not enough information is available, the screener should select the attribute with the highest risk. The number of times a screener is uncertain about which attribute to select should be minimal.

4.2 Page One of the DCF

The first page of the DCF includes tunnel identification, historical information about the tunnel, and target density. Tunnel identification is especially important when a group of tunnels are assessed. The electronic version of page 1 is shown in Figure 4-1, and the paper version is shown in Figure 4 2.

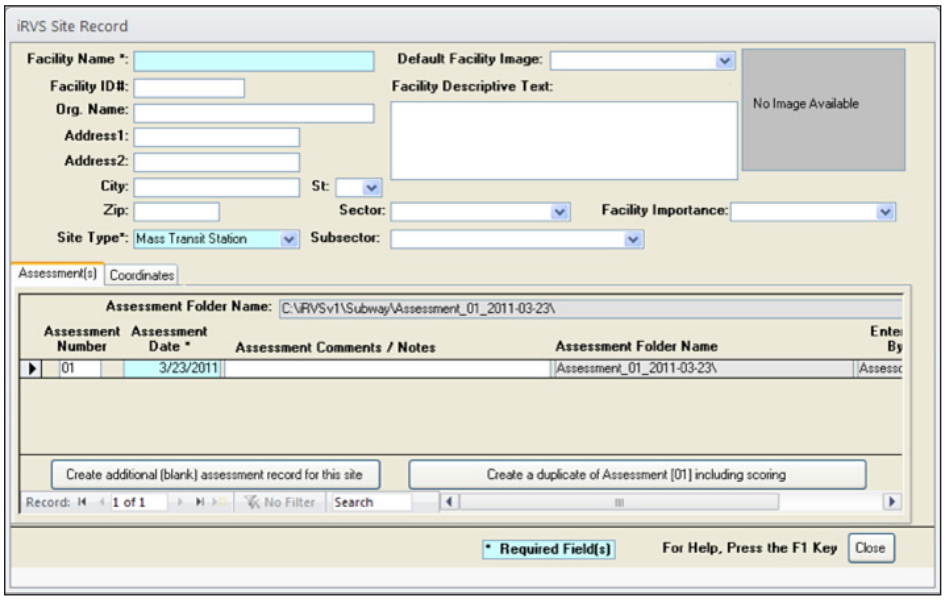


Figure 4-1:
Data Collection Form, page 1

Pre-Field Information

Complete the information on this page before the field assessment, using additional sheets as needed. The numbers in parentheses refer to the ID number in the catalog. Refer to the catalog for explanations of the information that is requested on this page and the potential sources of the information.

Station name/identification _____

Address/intersection _____

Transit agency _____

Year built _____ Footprint (in square feet) _____

Overview of the station from the transit agency _____

_____

_____

_____

Number of tracks (1.1) _____ Number of levels (1.2) _____

Station elevation (1.3) _____ Replacement value (1.10) _____

Peak daily ridership/transfers (1.4) _____

Terrorist threats against the station (2.3) _____

_____

Terrorist threats against the transit system (2.4) _____

_____

History of flooding affecting the station since opening(2.11) _____

_____

Geology: Soil conditions (3.9) _____

Year(s) of major retrofits (5.3) _____

Retrofit description _____

Operating hours (12.8) _____

Target Density. Number of potential high-value/CIKR targets/buildings within 300 feet and between 300 and 1000 feet of any point of the perimeter of the station (1.7).

CIKR Sector	Within 300 feet	From 300 to 1000 feet
Agriculture and Food		
Banking and Finance		
Chemical		
Commercial Facilities		
Communications		
Critical Manufacturing		
Dams		
Defense Industrial Base		
Emergency Services		
Energy		
Government Facilities		
Healthcare and Public Health		
Information Technology		
National Monuments/Icons		
Nuclear Reactors, Materials, and Waste		
Postal and Shipping		
Transportation Systems		
Water		
TOTAL		

Figure 4-2: Data Collection Form (paper version), page 1

4.3 Step One: Consequences Rating

4.3.1 Consequence Ratings Characteristics

Consequences are related primarily to the use, occupancy (the function of the building or infrastructure), and importance of the tunnel from the owner's perspective. Rating consequences involves assessing the following tunnel characteristics:

- Number of tracks / lanes
- Number of levels
- Underwater tunnel
- Peak number of travelers per day
- Tunnel locality

- Nearby or adjacent transportation systems / public assembly facility
- High-value targets / critical infrastructures
  - Within 300 feet
  - Between 300 feet and 1000 feet
- Impact of physical loss / criticality
  - Station
  - Track
- Social impact
- Replacement value
- Operational redundancy
- Estimated down time after a large disaster

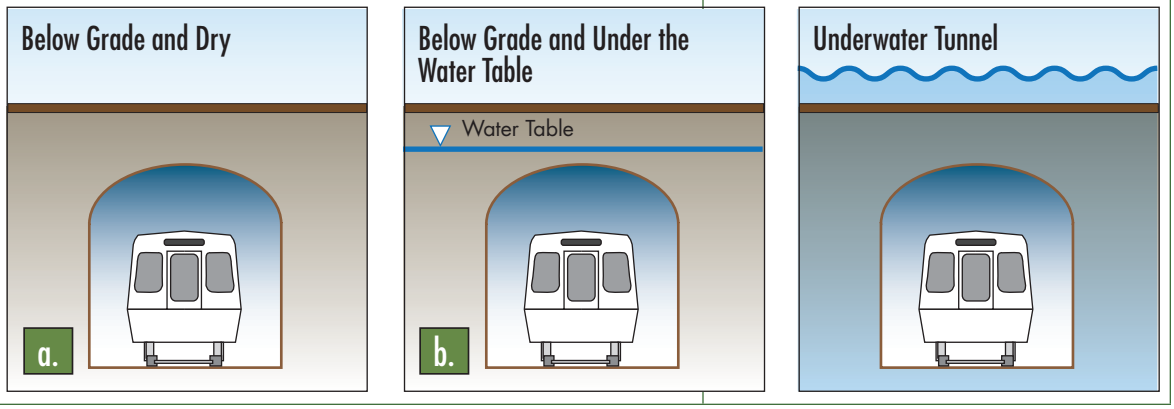
Information used to determine the consequence rating typically comes from the owner/operator, government sources, municipalities, and publicly accessible sources. This information should be gathered before the field assessment or during interviews with key personnel (see Section 3.2.1).

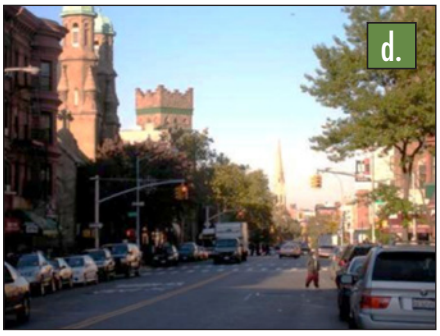
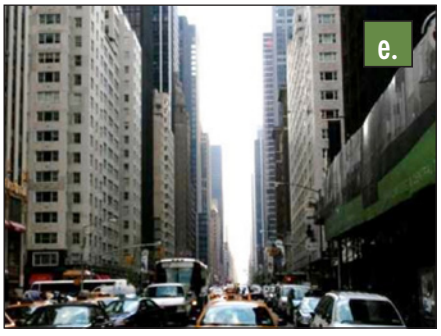
Information used to determine the consequence rating typically comes from the owner/operator, government sources, municipalities, and publicly accessible sources.

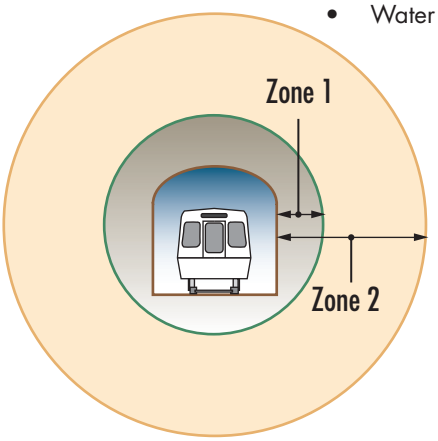
4.4.2 Catalog of Tunnel Characteristics and Attribute Options for the Consequence Rating

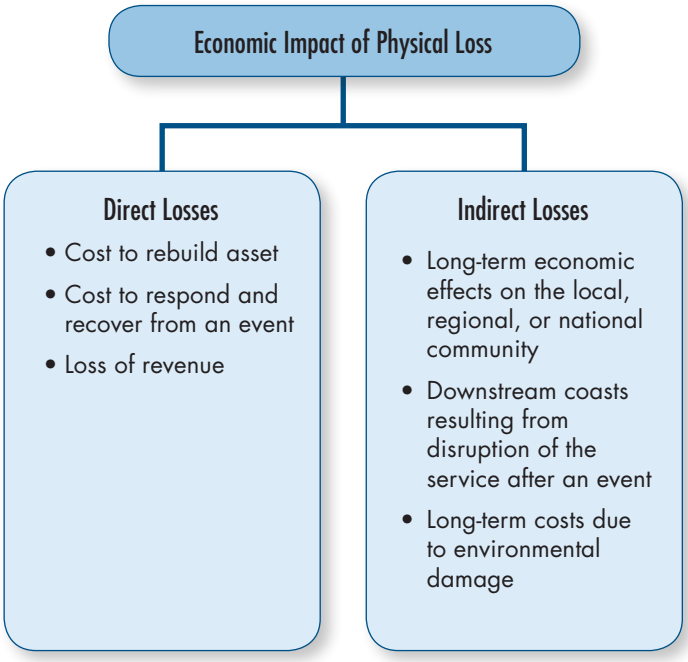
The catalog of consequence characteristics and attribute options is provided in Table 4 1. The catalog is also part of the IRVS database. The ID number in the catalog corresponds to the number of the characteristic in the DCF. The screener should use the catalog as a reference, as needed, when evaluating the characteristics.

Table 4-1: Catalog of Tunnel Characteristics and Attribute Options for the Consequences Rating

1. Consequence Rating		
ID	**Tunnel Characteristics**	**Attribute Options**
1.1	**Number of Tracks or Lanes** Number of tracks or lanes in the tunnel including all tubes or bores.	a. 1 b. 2 c. 3 to 4 d. 5 to 8 e. More than 8
	 *b. Two-track rail tunnel.*	 *c. Four-lane interstate highway tunnel*
1.2	**Tunnel Medium** The condition surrounding the tunnel (i.e., water or soil). The most common type of tunnel medium is below grade (surrounded by soil). Tunnels below grade can be constructed through dry soil or below the water table. Underwater tunnels provide a passage under a body of water for transportation systems (highways, railroads, and subways). Tunnels built through dry soil are expected to have lower consequences than tunnels surrounded by water. If an underwater tunnel is breached or damaged, the flooding, fire, or smoke consequences in the tube would be significant.	a. Below grade (dry) b. Below grade (under water table) c. Underwater
		

1. Consequence Rating		
ID	**Tunnel Characteristics**	**Attribute Options**
1.3	**Peak Number of Travelers per Day** Number of people who travel through the tunnel on a peak day. Most mass transit authorities provide traveler reports to the public on the Internet. The screener should research this characteristic during the pre-field assessment. When ridership information is not available, the screener will have to estimate the number of riders per day.	**Low ridership (in riders per day):** a. Less than 1,000 b. 1,000 to 2,000 c. 2,000 to 5,000 d. 5,000 to 10,000 e. 10,000 to 20,000 **High ridership (in riders per day):** f. 20,000 to 50,000 g. 50,000 to 100,000 h. 100,000 to 150,000 i. 150,000 to 200,000 j. More than 200,000
1.4	*Locality of Tunnel* Population density and land use surrounding the tunnel. The screener should consider the time of day the activity in the locality is at its peak. For instance, the peak activity in a business district may occur during the morning rush hour; this location should be described as urban or dense urban. The attribute options are listed from lowest (Option A) to highest risk (Option E). When the tunnel spans more than one type of locality, the screener should select the more conservative option (higher risk).  *d. Dense urban neighborhood and street above a mass transit tunnel*  *e. Dense urban street over a four-track mass transit tunnel*	**Least Risky** a. **Remote.** Sparsely populated with very few inhabitants. In major urban areas, remote would describe primarily rights-of-way that travel through parkland or protected areas that are off-limits to development. b. **Rural.** Low ratio of inhabitants to open land or farmland or an outlying part of a city or town. c. **Suburban.** Small town or city with low population density or mixed-use office park, warehouse, and manufacturing. d. **Urban.** Metropolitan area in a city or large town. e. **Dense urban.** Densely populated area in a major urban corridor where there are clusters of commercial, retail, and residential buildings located on congested streets. In these situations there is a significant chance of collateral consequences to populations, on the streets and in surrounding structures. **Most Risky**

1. Consequence Rating		
ID	**Tunnel Characteristics**	**Attribute Options**
1.5	***Adjacent/Nearby Transportation Systems or Public Assembly Venues*** Any transportation system (tunnels, structures, or modes) or public assembly venue that is above, below, or within 300 feet of the tunnel. Bus stops are not included. Public assembly venues include: • Amphitheater • Arena • Convention center • Museum • Performing arts center / auditorium • Shopping mall • Stadium	a. **None.** No other transportation systems or public assembly venues are within 300 feet of any part of the tunnel. b. **Close.** Another transportation system or public assembly venue is within 300 feet of the tunnel but is not connected. c. **Tightly integrated.** The tunnel is connected to either another transportation system or a large public assembly facility through tunnels, passageways, the structure, or other connection.
1.6	**High-Value/CIKR Targets** A high-value/CIKR target is any structure or asset the incapacitation or destruction of which would have a debilitating impact on the security, economy, public health or safety, and/or environment across any Federal, State, regional, territorial, or local jurisdiction. The 18 Critical Infrastructure and Key Resources (CIKR) sectors defined by DHS for evaluating target density are listed below and are available in the DCF and also in DHS (2009). Subsectors should also be reviewed for this characteristic. **CIKR Sectors** • Agriculture and Food • Banking and Finance • Chemical • Commercial Facilities • Communications • Critical Manufacturing • Dams • Defense Industrial Base • Emergency Services • Energy • Government Facilities • Healthcare and Public Health • Information Technology • National Monuments and Icons • Nuclear Reactors, Materials and Waste • Postal and Shipping • Transportations Systems • Water  **Zone 1**– Within 300 feet of the perimeter of the structure **Zone 2** – Within 1,000 feet of the perimeter of the structure	High-value/CIKR targets are divided into two zones for this characteristic according to the distance of the target from any point of the perimeter of the tunnel. Zone 1 is within 300 feet of any point of the perimeter of the tunnel, and Zone 2 is between 300 feet and 1,000 feet of any point of the perimeter of tunnel. In most cities, 300 feet is equal to approximately 1 block, and 1,000 feet is equal to approximately 3 blocks. **Zone 1.** Number of targets within 300 feet of any point of the perimeter of the tunnel. a. None b. 1 to 6 c. 7 to 12 d. 13 to 19 e. 20 or more **Zone 2.** Number of targets between 300 feet and 1,000 feet of any point of the perimeter of tunnel. a. None b. 1 to 6 c. 7 to 12 d. 13 to 19 e. 20 or more

1. Consequence Rating		
ID	**Tunnel Characteristics**	**Attribute Options**
1.7	**Impact of Physical Loss/Criticality** Extent to which loss of or serious damage to the tunnel would affect the livelihood and resources of individuals and businesses in the local, regional, and national community. Criticality refers to the importance of the tunnel to the system or region. Partial or complete physical loss of a tunnel from a terrorist attack or natural disaster would have direct and/or indirect economic consequences. Direct loss includes the cost to rebuild an asset and cost to respond to and recover from the even. Indirect loss includes the costs resulting from the disruption of a product or service and the long-term costs from environmental damage. The impact of physical loss includes consequences from the loss of a facility above the tunnel. For this characteristic, the economic impact of physical loss should be evaluated for two scenarios: • Loss of the tunnel • Loss of the tracks or lanes The difference between the impact of physical loss of the actual tunnel and the tracks or lanes is due to the direct and indirect losses associated with loss of the tunnel. The loss of the tunnel itself is asset-oriented and will have a direct impact. The loss of the tracks or lanes could result in indirect losses if the tracks or lanes are shared by multiple authorities, and a major corridor for multiple systems is interrupted. The attribute options define the geographic limits of the economic impact of the loss of a tunnel.  	a. **Local.** The tunnel has little, if any, importance to maintaining the transportation system's service levels, mobility with respect to the regional transportation system, and the local and regional economy. The regional transportation system would be minimally affected, and regional authorities would be able to route passengers around distressed areas easily. b. **Regional.** Loss of the tunnel would substantially affect the transportation system and force passengers to find alternative transportation, which would result in increased congestion-related environmental and employment costs locally and in the region. c. **National.** Loss of the tunnel would severely strain the regional transportation system, and movement around the region via other modes would be disrupted significantly, resulting in extreme social and economic costs nationally,

1. Consequence Rating		
ID	**Tunnel Characteristics**	**Attribute Options**
1.8	**Social Impact** Psychological effect on public morale and confidence in the transportation system. Social impacts of loss include the decrease in the public's mobility, lack of confidence in the transportation system, and environmental impacts. Included are changes in the public's sense of safety and well-being after a significant event and possible subsequent aberrant behavior.	a. **Low.** There will be little or no effect on daily life in the region served by the transporation system. b. **Moderate.** A substantial number of people will stop using the transporation system. c. **High.** Transporation use in the affected region will be severely disrupted.
1.9	**Replacement Value (Fair Market Value)** Current market cost to construct a tunnel. Replacement value depends on the construction costs in the region. Replacement value information is obtained before the field assessment and is on page 1 of the DCF. This information should be obtained from a knowledgeable tunnel representative. If this is not possible, the value must be estimated using qualitative guidance for construction costs.	a. Less than $1 million (m) b. $1 m to $5 m c. $5 m to $20 m d. $20 m to $50 m e. $50 m to $100 m f. $100 m to $200 m g. $200 m to $350 m h. $350 m to $600 m i. $600 m to $900 m j. More than $900 m
1.11	**Operational Redundancy** The degree to which a transportation system is able to maintain a reasonable service level by routing passengers around a distressed tunnel, either by sharing tracks with other lines, bussing, or some other means of transportation for mass transit tunnels and providing an alternate route for highway tunnels.	a. **Very high.** Few, if any, disruptions would result from a problem in the tunnel, and transportation services or travelers would easily be re-routed. b. **High.** Some travelers would be affected, but most transportation operations would be able to continue, with service routed around the troubled tunnel without any disruptions. c. **Moderate.** Many travelers would be affected, but the transportation system would be functional with few delays for the majority of travelers. d. **Low.** Few, if any, alternative routes exist; failure of the tunnel would cause system delays, nearly crippling transportation operations. e. **Very low.** Failure of the tunnel would cripple transportation in the region and cause transportation operations to halt.

1. Consequence Rating		
ID	Tunnel Characteristics	Attribute Options
1.12	**Estimated Downtime after a Large Disaster** **Resiliency.** The amount of time needed for the tunnel to be restored and become operational after a disaster. A large disaster is considered an incident with the potential of causing catastrophic losses in terms of injuries, casualties, and damage.	a. **Very short.** Less than a day b. **Short.** Less than a week c. **Moderate.** Less than a month d. **Long.** Less than a year e. **Very long.** More than a year

4.5 Step Two: Threat Rating

This section contains (1) a description of the station characteristics that are assessed to determine the threat rating and (2) the catalog of threat characteristics and attribute options.

4.5.1 Threat Rating Characteristics

The threat rating is a function of the following transit station characteristics:

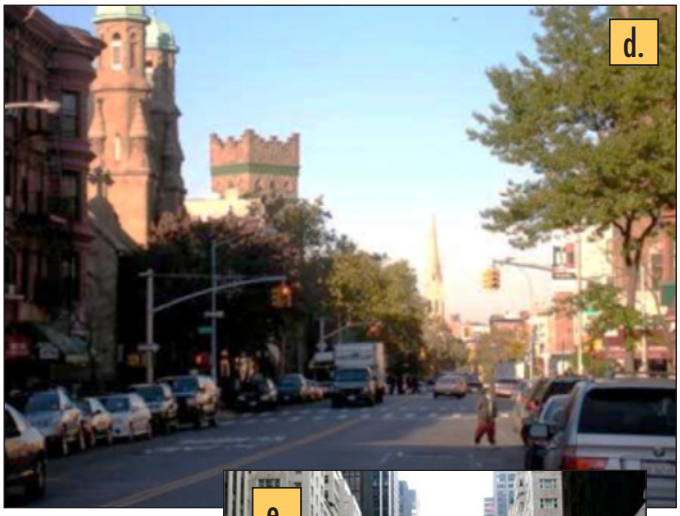
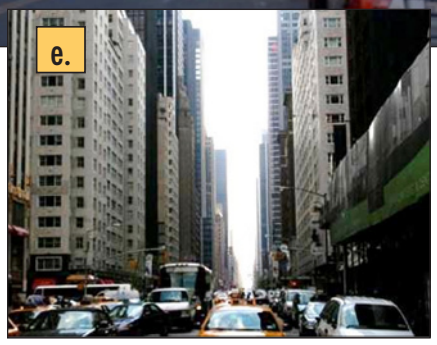
- Station locality
- Peak number of riders/transfers per day
- History of planned, thwarted, or successful terrorist attacks
  - Station
  - Transit system
- High value targets/CIKR
  - Zone 1 (within 300 feet of the station)
  - Zone 2 (between 300 and 1,000 feet of the station)
- Significance of station
- Function criticality within the system/region
- Number of entrances/exits
- Plaza/public areas
- Protective deterrence measures
- Accessibility of off-duty vehicles/equipment
- Flooding history

The transit station characteristics that are the same for the consequence and threat ratings are station locality, peak number of riders/transfers, and high-value targets/CIKR. In the IRVS database, these characteristics are automatically selected after they are input in the consequence section of the DCF.

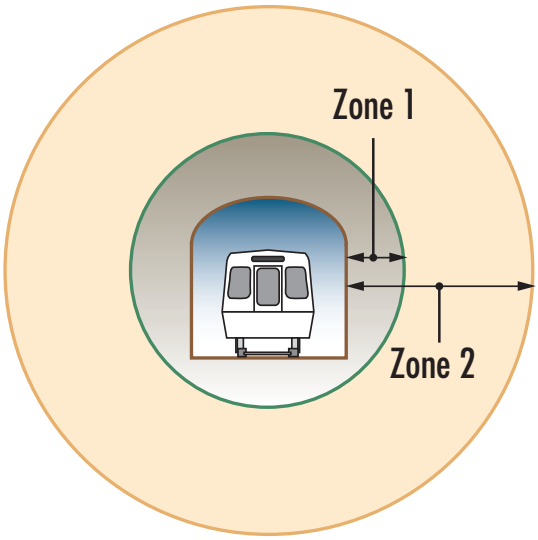
4.5.2 Catalog of Tunnel Characteristics and Attribute Options for the Threat Rating

The catalog of threat characteristics and attribute options is provided in Table 4 2. The catalog is also provided electronically the IRVS database. The ID number in the catalog corresponds to the number of the characteristic in the DCF. The screener should use the catalog as a reference, as needed, when evaluating the characteristics on the DCF.

Table 4-2: Catalog of Tunnel Characteristics and Attribute Options for the Threat Rating

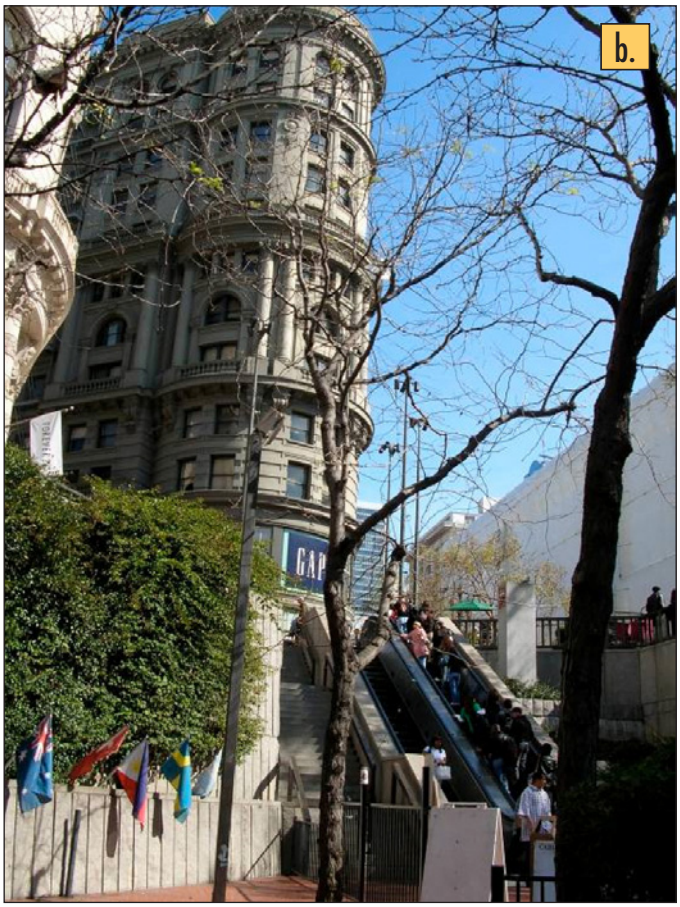
2. Threat Rating		
ID	**Tunnel Characteristics**	**Attribute Options**
2.1	**Tunnel Locality** Population density and land use surrounding the tunnel . The screener should consider the time of day the activity in the locality is at its peak. For instance, the peak activity in a business district may occur during the morning rush hour; this location should be described as urban or dense urban. When the tunnel spans more than one type of locality, the more conservative option (higher risk) should be selected.   *d. Dense urban neighborhood and street above a mass transit tunnel.* *e. Dense urban street over a four-track mass transit tunnel.*	**Least Risky** a. **Remote.** parsely populated with very few inhabitants. In major urban areas, remote would describe primarily rights-of-way that travel through parkland or protected areas that are off-limits to development. b. **Rural.** Low ratio of inhabitants to open land or farm land, or an outlying part of a city or town. c. **Suburban.** Small town or city with low population density or mixed-use office park, warehouse, and manufacturing. d. **Urban.** Metropolitan area in a city or large town. e. **Dense urban.** Densely populated area in a major urban corridor where there are clusters of commercial, retail, and residential buildings located on congested streets. In these situations there is a significant chance of collateral consequences to populations, on the streets and in surrounding structures. *Most Risky*

2. Threat Rating		
ID	**Tunnel Characteristics**	**Attribute Options**
2.2	**Peak Number of Travelers per Day** Number of people who travel through the tunnel on a peak day. Most mass transit authorities provide ridership reports to the public on the Internet. The screener should research this characteristic during the pre-field assessment. When traveler information is not available, the screener will have to estimate the number of riders per day.	**Low number of travelers (per day):** a. Less than 1,000 b. 1,000 to 2,000 c. 2,000 to 5,000 d. 5,000 to 10,000 e. 10,000 to 20,000 **High number of travelers (per day):** f. 20,000 to 50,000 g. 50,000 to 100,000 h. 100,000 to 150,000 i. 150,000 to 200,000 j. More than 200,000
2.3	**Terrorist Threats (Credible)** A terrorist threat refers to any planned, thwarted, or successful attack against the tunnel or transportation system in the past or present. This characteristic addresses the likelihood of a terrorist attack occurring at the tunnel under consideration. Unsubstantiated threats, such as called-in bomb threats, should not be considered. To determine whether a threat is credible, the screener should obtain the most accurate threat information and talk to a senior security representative for the tunnel or transportation authority. Information may also be available from law enforcement officials in the area, newspapers, and the Internet. The screener may have to use judgment based on the best available information at the time of the screening.	
2.3.1	**Terrorist Threats: Tunnel** Any credible threat, past or present, to the tunnel.	a. No b. Previous c. Current
2.3.2	**Terrorist Threats: Transportation System** Any credible threat to the transportation system operating the tunnel. If a credible threat has been made to a transportation system (e.g., Washington Metro), but no particular tunnel has been identified, the threat should be counted.	a. No b. Previous c. Current

2. Threat Rating		
ID	**Tunnel Characteristics**	**Attribute Options**
2.4	**High-Value/CIKR Targets** A high-value/CIKR target is any structure or asset the incapacitation or destruction of which would have a debilitating impact on the security, economy, public health or safety, and/or environment across any Federal, State, regional, territorial, or local jurisdiction. The 18 Critical Infrastructure and Key Resources (CIKR) sectors defined by DHS for evaluating target density are listed below and are available in the DCF and also in DHS (2009). **CIKR Sectors** • Agriculture and Food • Banking and Finance • Chemical • Commercial Facilities • Communications • Critical Manufacturing • Dams • Defense Industrial Base • Emergency Services • Energy • Government Facilities • Healthcare and Public Health • Information Technology • National Monuments and Icons • Nuclear Reactors, Materials and Waste • Postal and Shipping • Transportations Systems • Water  **Zone 1**– Within 300 feet of the perimeter of the structure **Zone 2** – Within 1,000 feet of the perimeter of the structure	High-value/CIKR targets are divided into two zones for this characteristic according to the distance of the target from any point of the perimeter of the tunnel. Zone 1 is within 300 feet of any point of the perimeter of the tunnel, and Zone 2 is between 300 feet and 1,000 feet of any point of the perimeter of tunnel. In most cities, 300 feet is equal to approximately 1 block, and 1,000 feet is equal to approximately 3 blocks. **Zone 1.** Number of targets within 300 feet of any point of the perimeter of the tunnel. a. None b. 1 to 6 c. 7 to 12 d. 13 to 19 e. 20 or more **Zone 2.** Number of targets between 300 feet and 1,000 feet of any point of the perimeter of tunnel. a. None b. 1 to 6 c. 7 to 12 d. 13 to 19 e. 20 or more

2. Threat Rating		
ID	**Tunnel Characteristics**	**Attribute Options**
2.5	**Significance of Tunnel** Symbolic nature or landmark status of the tunnel. If the tunnel is on a national, State, local, or nongovernmental historic registry, the screener should select either Option C or Option D. The screener can determine whether the tunnel is on an historic registry by: • Consulting with the transit authority or building management • Reviewing the National Register of Historic Places at www.nationalregisterofhistoricplaces.com • Checking with States, local jurisdictions, and non-governmental organizations for listings of historically significant buildings within a locality • Checking the outside of the station or building in which the station is housed for a plaque indicating its status as an historic property.  *c. The Holland Tunnel in New York City, which is on the U.S. National Register of Historic Places and a National Historic Landmarkb. Station with regional significance*	a. **Local.** The tunnel is recognizable only to locals and can be confused with similar tunnels. The tunnel has no media value or symbolism for the public. b. **Regional.** The tunnel is recognizable only to people in the State and region. The tunnel is prominent in the local community and is a local landmark. The tunnel has some media value on a regional level. c. **National.** The tunnel is easily recognizable and is featured in the national mass media. The tunnel is considered a landmark and is located in an architecturally significant structure. d. **International.** The tunnel is easily recognizable and is featured in international mass media. An example is the Chesapeake Bay Bridge Tunnel, considered one of the seven engineering wonders of the modern world.

2. Threat Rating		
ID	**Tunnel Characteristics**	**Attribute Options**
2.6	**Function Criticality within a Transportation System or Region** Function criticality describes the importance of a tunnel to the regional transportation system. When a tunnel is used heavily but has redundancy with other transportation systems, it should be rated lower.	a. **Very low.** The regional transportation system would barely be affected by loss of the tunnel, and regional authorities would easily be able to route passengers around distressed areas. b. **Low.** Loss of the tunnel would result in delays in the regional transportation system, and passengers would have longer commutes, but regional transportation mobility would not be severely affected. c. **Moderate.** Loss of the tunnel would cause significant delays in the regional transportation system, but movement around the region would continue. d. **High.** Loss of the tunnel would severely strain the regional transportation system, and movement around the region via other modes would be disrupted significantly. e. **Very high.** The regional transportation system has no redundancy to compensate for the loss of the tunnel; transportation operations around the region would nearly cease, for example, when station is a regional or a multimodal transportation hub.
2.7	**Number of Approaches** Number of direct tracks or lanes of access by trains and/or vehicles to a tunnel.	a. 1 to 2 b. 3 to 4 c. 5 to 8 d. 9 to 12 e. More than 12

2. Threat Rating		
ID	**Tunnel Characteristics**	**Attribute Options**
2.8	**Plaza/Public Area** A plaza is an open public space outside the controlled access to the tunnel. The plaza can be at grade or below grade and sometimes has public seating and seating areas. Plaza's provide a pleasant space for people to relax, converse, and enjoy the outdoors in a more spacious setting; however, if not properly designed, plazas can leave the tunnel susceptible to an attack. Barriers and landscape features should be designed to make the plaza impenetrable for a vehicle. Furthermore, the plaza should be under surveillance using cameras and/or patrols.  *b. Below-grade public plaza leading to a transit entrance with numerous obstacles between traffic and the transit entrance*	a. **None.** No plaza/public area. b. **Well-controlled.** Numerous barriers that are well-positioned to obstruct vehicular entry and regular surveillance. c. **Moderate control.** Some vehicular barriers but several notable security flaws (e.g., temporary or ornamental barriers that can easily be defeated by vehicles). d. **Not controlled.** No vehicular barriers or surveillance.  *c. Public plaza with some protection*  *d. Public area adjacent to a subway station without limited access management controls*

2. Threat Rating		
ID	**Tunnel Characteristics**	**Attribute Options**
2.9	**Protective Deterrence Measures** Visibility and/or prominence of protective security measures that discourage an aggressor from attacking the tunnel. Security creates a psychological deterrent for an aggressor who is considering attacking the tunnel. Visibility inhibits criminal behavior because of the fear of being caught. A potential aggressor who perceives a risk of being caught may be deterred from attacking the tunnel. For deterrence to be effective, security measures should be prominent and visible throughout the tunnel (i.e., perimeter, site, and tunnel interior). Combined security measures, such as those listed below, may be used in all areas of the tunnel: • Security guards (armed and unarmed) • Law enforcement patrols • Monitoring and surveillance equipment • Dedicated search and screening • Random search and screening • Mobile screening (e.g., canine unit) • Access controls • Public awareness and notification of protective measures	a. **High.** Security measures are prominent and visible in all areas of the tunnel (interior and exterior). b. **Medium.** Security measures are prominent and visible only in one or two areas of the tunnel. For instances, security measures may be prominent inside the tunnels but not at the perimeter. c. **Low.** Security measures are minimal or not visible enough to discourage an attacker in any area of the tunnel. An attacker would not be discouraged by the security measures from attacking the tunnel.
2.10	**Flooding History** Flooding refers to an incident in which the tunnel was unable to clear water in a timely manner during a water surge. Service on rail systems can be disrupted by flooding from both major and minor rainstorms. Rainwater can disrupt signals underground and can require the electrified third rail be shut off. The screener should research historical data of flooding at the tunnel through open sources back when the tunnel opened.	a. **None.** No record of flooding. b. **Limited.** Some flooding has occurred, but service was either not disrupted or quickly restored. d. **Moderate.** Flooding has occurred often, causing disruptions. e. **Severe.** Flooding has impaired operations for significant periods.

4.6 Step Three: Vulnerability Rating

4.6.1 Vulnerability Rating Characteristics

The vulnerability rating is a function of tunnel characteristics that may be adversely affected by a terrorist attack, natural hazard, or accidental event.

The vulnerability rating characteristics are:

- Site
- Architecture
- Structure
- Ventilation (including HVAC)
- Fire protection
- Operations (e.g., power supply, lighting)
- Nonstructural components
- Physical security
- Cyber infrastructure
- Operational security

4.6.1.1 Site

Site vulnerability refers to the condition of the area between the approaches of the tunnel and the area above and adjacent to the tunnel.

4.6.1.2 Architectural

Architectural considerations involve the tunnel layout and space design. Space design relates to separating public areas of the tunnel from the more secured areas of the facility. Features such as the number of entrances, number of levels, service entrances, lobby/lobbies, retail space, and integrated/adjacent parking garages are key characteristics of architectural vulnerabilities. Furthermore, the number of levels and tracks in the tunnel are critical to the overall vulnerability.

4.6.1.3 Structural

Structural vulnerability is defined as a weakness in a structure's ability to supports its own weight and the weight of its contents and to resist loads from wind and earthquake. Structural vulnerabilities can be exploited by an aggressor. Evaluating structural vulnerabilities is limited by the extent to which the structure is covered with finishes. The structural framing in public areas is typically covered for aesthetic purposes making it difficult to determine the materials underneath the finishing.

To identify the structural characteristics as accurately as possible, the following steps should be taken before the field assessment:

- Review the structural as-built drawings, including renovations/retrofits. Drawings provide the most detailed structural information.
- Make arrangements to talk to the tunnel engineer during the field assessment.
- Request permission to tour areas without interior finishes or areas not accessible by the public.

Reviewing the drawings and questioning the tunnel engineer may be the most efficient way to assess the structural vulnerability. Site observation can be more time-consuming but is necessary when the drawings are not available.

The structural characteristics that are evaluated have a strong influence on a tunnel's performance in a terrorist attack or natural disaster. Structural vulnerability to an explosive event is dependent on the magnitude of the air blast shock wave as it loads walls, columns, and floor/framing.

4.6.1.4 Ventilation

Ventilation refers to any system that permits air intake or exhaust to control temperature or remove moisture, odors, smoke, heat, dust, and airborne bacteria. Ventilation systems are also referred to as HVAC systems. Ventilation systems are required in tunnels because of heat from the railway tunnels, fire hazards, exhaust from vehicles, and the potential for CBR threats. All building structures that are served by the ventilation systems in the tunnel are included in the IRVS.

Vulnerability is dependent on the exposure, protection, and redundancy of HVAC systems. The likelihood of a CBR contaminant being introduced in the tunnel is greatly influenced by the accessibility of the air vents to the public.

Ventilation systems are more applicable to vehicle tunnels than rail tunnels because of the high concentration of contaminants in vehicular tunnels. Rail tunnels often have ventilation systems in the stations or at intermediate fan shafts but during normal operating hours rely on the piston effect of trains pushing air through the tunnel to remove stagnant air. Many rail tunnels have emergency mechanical ventilation that works only in the event of fire (FHWA, 2005).

Ventilation system characteristics are given significant weight in the vulnerability rating for CBR threat scenarios.

4.6.1.5 Fire Protection System

A fire protection system is any system that prevents or suppresses a fire and/or provides protection in a fire. Fire protection systems include fire and smoke-detection alarms and fire suppression. Life safety in the tunnel is supported by the fire protection systems by warning people to evacuate, allowing for safe evacuation by maintaining life safety, and suppressing the fire before firefighters arrive. Figure 4-3 shows an example of an innovative fire protection system, known as the "Tunnel Plug," currently under development and funded by DHS S&T.

A fire protection system has eight subsystems:

- Detection
- Alarm
- Verification
- Incident location
- Communications
- Response plan
- Personnel evacuation
- Smoke control (ventilation)

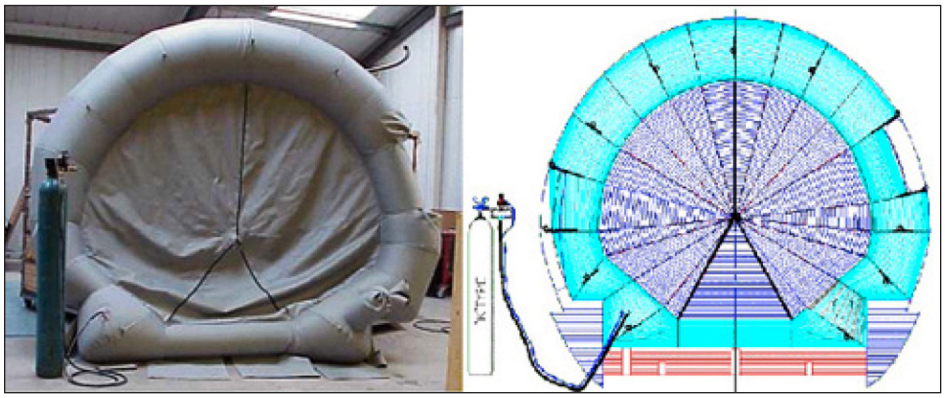


Figure 4-3:
The "Tunnel Plug" is an example of an innovative fire suppression system under development for tunnels. Funded by DHS S&T, the plug is designed to drop from the ceiling and inflate inside the tunnel, essentially sealing off the passageway and preventing smoke or fire from spreading.

4.6.1.6 Operational Systems

Operations refer to the critical utility and control functions required for the transit station to operate safely and efficiently (e.g., power supply, lighting, monitoring, surveillance).

4.6.1.7 Nonstructural

Nonstructural vulnerabilities are vulnerabilities in non-load-bearing features (e.g., wall and ceiling finishes, fixture attachments, police booths, barriers).

4.6.1.8 Physical Security

Physical security refers to any method or system whose purpose is to detect, prevent, and protect against any threat or hazard. The availability and effectiveness of security-related detection systems are the key concerns in physical security vulnerabilities.

The vulnerability assessment of physical security begins by reviewing the available security detection systems in the transit station and evaluating the effectiveness of the collective systems. The purpose is to assess the ability of a given security system to prevent a threat from being carried out.

Security personnel should be interviewed before or during the field assessment. Reviewing security system documentation is also recommended. If no interview is conducted, at least one screener on the IRVS team should have a basic understanding of security principles.

4.6.1.9 Cyber Infrastructure

Cyber infrastructure includes electronic information, control systems, and/or communication systems needed for daily operations. Cyber infrastructure is critical to the functions and services of a tunnel. Because cyber infrastructure is interconnected, attacks using cyber tools can spread quickly and have debilitating effects. Cyber vulnerabilities are addressed through evaluation of communication and control systems of the tunnel.

Security and information technology personnel should be interviewed during the field assessment. Review cyber-security system documentation is also recommended.

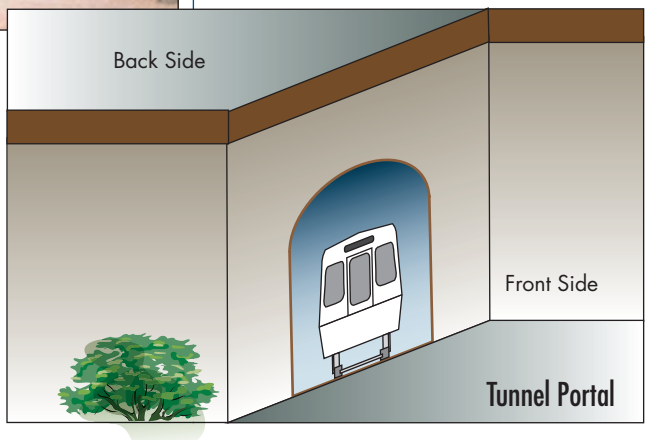
4.6.1.10 Operational Security

Operational security refers to the transit agency's emergency preparedness and planning for the tunnel. Operational security vulnerabilities are assessed by evaluating emergency and security response plans, mass evacuation plans, and training of emergency response personnel.

4.6.2 Catalog of Tunnel Characteristics and Attribute Options for the Vulnerability Rating

The catalog of vulnerability characteristics and attribute options is provided in Tables 4 3a through 4 3j. The catalog is also provided electronically in the IRVS database. The ID number in the catalog corresponds to the number of the characteristic in the DCF. The screener should use the catalog as a reference, as needed, when completing the DCF.

Table 4-3a: Catalog of Tunnel Characteristics and Attribute Options for Site Vulnerabilities

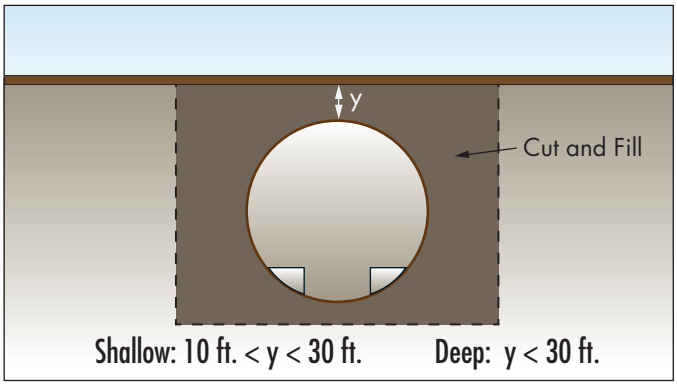
3. Vulnerability Rating: Site Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
3.1	**Tunnel Maintenance/Service Facility** This facility controls all electrical feeds (both high- and low-voltage supplies) into the tunnel or section of tunnel (single or redundant) and other vital equipment to maintain tunnel operations (such as ventilation and fire suppression systems). The tunnel may have more than one of these facilities depending on its size (area). If the tunnel service building is seriously damaged, the tunnel would be unsafe and would be closed for a considerable period, causing major disruption. Most major highway tunnels have more than one of maintenance/service facility. In a subway tunnel, the system's tunnels normally serve as the maintenance/service facilities.	a. Available/redundant b. Some availability/some redundancy c. Available/not redundant d. Not available/not redundant
3.2	**Portals** Any point at which a tunnel transitions from tunnel to open air.  a. Portal protected by buildings and cladding  *a. Back of portal protected by bollards, fencing, and barbed wire* 	a. Protected b. Exposed front c. Exposed back d. Underwater

3. Vulnerability Rating: Site Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
3.2	**Portals (continued)**  *b. Front of portal exposed to both intentional and accidental impacts.*	 *c. Back of a portal exposed to both intentional and accidental impacts*
3.3	**Tunnel Approaches** Direct tracks and lanes of tunnel access and egress for trains and/or vehicles.  *a. Approach to a highway tunnel*	a. More than 3 b. 2 to 3 c. Only 1  *b. Approach to a railway tunnel*

3. Vulnerability Rating: Site Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
3.4	**Presence of Stand Pipes / Fire Hydrants (Water Supply)** A standpipe is a type of rigid water piping that is built into a tunnel in a vertical or horizontal position. Fire hoses can be connected to the piping, allowing manual application of water to the fire. Some tunnels may have fire hydrants near the approaches. The presence of standpipes and/or fire hydrants in the tunnel should be used to evaluate the adequacy of water supply to the tunnel. The availability and sufficiency of water provided to the tunnel is critical for general operations such as fire protection.	a. Yes b. No  *a. Standpipe at the portal of the tunnel where fire hoses can be connected*
3.5	**Water Drainage** Adequate water drainage allows the tunnel to clear water in a timely manner during a water surge. Service on a transportation tunnel may be disrupted by flooding of only a few inches. Water drainage should be evaluated by inspection of the drainage structures, pump room (when present), and research of historical data of flooding in the tunnel.  *c. A poor drain clogged with debris that can limit the tunnel's ability to clear water in a timely manner.*	a. **Excellent.** The tunnel controls water inflow well, and flooding does not impede transit operations. b. **Moderate.** Some flooding has occurred, but service was either not disrupted or quickly restored. c. **Limited.** Flooding has impaired operations for limited periods. d. **Deficient.** Flooding has impaired operations for significant periods.

3. Vulnerability Rating: Site Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
3.6	**Natural Protective Barriers** Natural protective barriers are terrain elements such as grassy knolls, hills, ditches, boulders, shrubs, trees, or water bodies that make traversing a site difficult or may at least delay an aggressor. An assessment of natural protective barriers is an assessment of the degree to which a tunnel is shielded from unwanted entry or malicious acts.	a. **Not applicable** b. **High.** Tunnel portals and assets are surrounded by natural features that make a close approach by unwarranted vehicles or aggressors nearly impossible. The tunnel's designers have incorporated the principles of Crime Protection Through Environmental Design. c. **Medium.** Tunnel portals and assets have natural features that create obstacles to approaching vehicles or aggressors. Approaching the tunnel by vehicle or on foot is difficult but not impossible. d. **Low.** The tunnel and assets have little or no protection from aggressors or vehicular attack, either accidental or intentional.
3.7	**Manmade Barriers** Manmade features are structural protective barriers such as bollards, fencing, walls, floors, roofs, bars, and roadblocks that are used to restrict, channel, or impede access and provide standoff distance between the tunnel and the public / vehicles. These barriers are designed to deter threats and delay the undeterred aggressor. An assessment of manmade barriers is an assessment of the degree to which a tunnel is shielded from intrusion and vehicles that can intentionally or accidently damage the tunnel. The screener evaluates this characteristic by assessing the presence and effectiveness of bollards/barriers and fencing at the site.	
3.7.1	**Barriers/Bollards** Physical wall or bollard to prevent intrusion of vehicles.  *Site partially protected by a brick wall, but without standoff or any other protective barriers, the site is fundamentally exposed.*	a. **Not applicable** b. **High.** Permanent barrier resistance to a 15,000-pound vehicle traveling at 50 mph with penetration of less than 3 feet. c. **Medium.** Permanent barrier resistance to a 15,000 pound vehicle traveling at 40 mph with penetration of less than 20 feet. d. **Low.** Fixed or movable barrier designed to limit or redirect vehicular access.

3. Vulnerability Rating: Site Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
3.7.2	**Fencing** Common means of establishing a physical protective barrier to protect a controlled area.  *Crash-rated fence (Ameristar Fence Products, Inc.)*	a. **Not applicable** b. **High.** Fence designed to provide optimal restriction or delay to pedestrian-based attacks. Vehicle and pedestrian gates are designed to continue the structural integrity of the fence line. • Double buried fence line • Height of 10 feet • Anti-climb/anti-cut fencing vertical bars with horizontal supports designed to make climbing difficult. • Top guard an overhang of barbed wire or tape along the top of the fence, facing outward and upward at an approximately 45-degree angle. • Hardened posts • Counter-sunk into concrete c. **Medium**. Fence designed to restrict or delay pedestrian-based attacks. Vehicle and pedestrian gates are designed to continue the structural integrity of the fence line. • Single buried fence line • Height of 10 feet • Hardened posts • Counter-sunk into concrete d. **Low.** Fence provides minimal delay to a pedestrian-based assault. • 7-foot chain-link fence
3.8	**Tunnel Medium** The conditions surrounding the tunnel (water or soil). Underwater tunnels provide a passage beneath a body of water for mass transit systems (highway, railroads, and subways). If an underwater tunnel is breached or damaged by an attack, the flooding, fire, or smoke consequences in the tube would be significant.	a. **Below grade (above water table).** Below the street level or prevailing natural features. b. **Below grade** (under water table) c. **Underwater.** Tunnel that is under a body of water.

3. Vulnerability Rating: Site Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
3.8	**Tunnel Medium (continued)**  *a. Busy street above a below-grade mass transit tunnel*	 *c. Vent shaft marking the site of an underwater tunnel*
3.9	**Depth of Cut and Cover above Tunnel** Depth of below-grade tunnel.  *Cross section illustrating the depth of cut and cover.*	a. **Not applicable.** Not constructed using cut and cover construction (e.g., drilled rock, immersed tube tunnels). b. **Deep.** More than 30 feet below grade. c. **Shallow.** 10 to 30 feet below grade. d. **Exposed.** 0 to 10 feet below grade with an open cut.

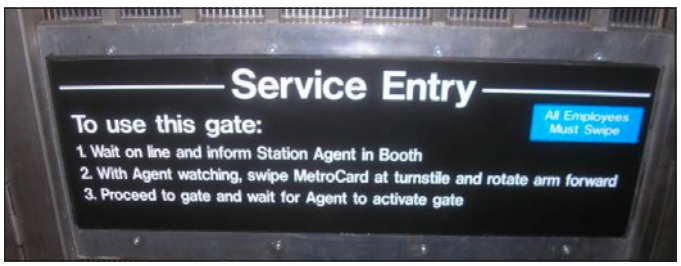
3. Vulnerability Rating: Site Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
3-10	**Geology (Soil Condition)** Geology, or soil condition, describes the type of soil/Geology, or soil condition, describes the type of soil/rock that a transit tunnel is built on or under. The geology surrounding the tunnels is critical to the framing and structure because it provides a substantial percentage of the load carrying capacity for underground structures. If the type of soil is not easy to identify, the screener should ask the transit authority.	a. **Hard rock** b. **Medium** c. **Poor** Note the following red flags in the DCF by checking the red flag and adding comments. • High water table • Presence of soft soils • Cut and fill • Evidence of slides or subsidence
3.11	**Adjacent Buildings** Applicable to any inhabited commercial, residential, Applicable to any inhabited commercial, residential, institutional, or industrial structure within 300 feet of the tunnel. Buildings that are used to support transportation operations, such as maintenance facilities and or transit parking garages, are not counted.	a. **None.** No adjacent buildings. Typical of this category are suburban locations with large commuter parking facilities and rural locations. b. **Some.** Some adjacent buildings. Typical of this category are urban and suburban neighborhoods with one- and two-story structures nearby. c. **Numerous.** Numerous adjacent buildings. Typical of this category are stations in dense urban neighborhoods, such as central cities or dense urban settings.

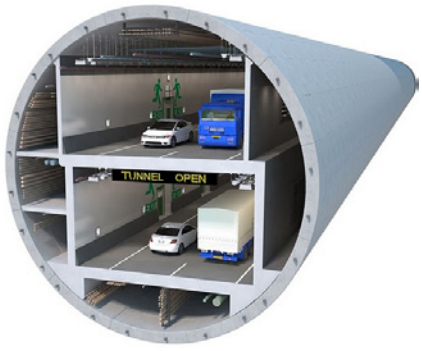
Soil Type	Suitability
Hard Rock	Best
Sand and Gravel	Medium
Medium and Hard Clays	Medium
Silts and Soft Clays	Poor
Organic Silt and Clays	Poor
Peat	Poor

c. Four-track mass transit tunnel below a street in a dense central business district with numerous buildings

3. Vulnerability Rating: Site Vulnerabilities		
ID	Tunnel Characteristics	Attribute Options
3.12	**Hazardous Materials Storage** Storage of hazardous materials in the tunnel or in surrounding areas poses a high risk to staff and riders because of the potential for combustion or release of lethal materials. Abundant open-source information on hazardous materials storage is available on Web sites such as the Environmental Protection Agency (EPA), State office of emergency management, and local fire department.	a. No b. Yes

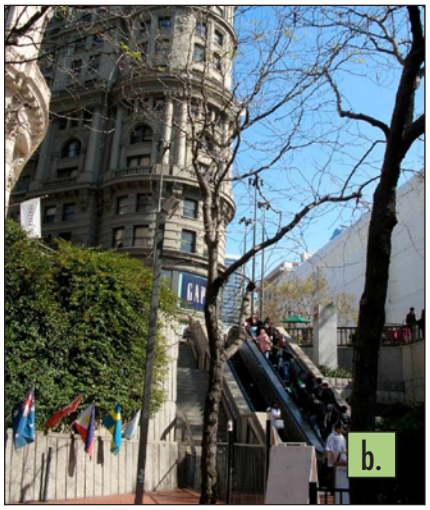
Table 4-3b: Catalog of Tunnel Characteristics and Attribute Options for Architectural Vulnerabilities

4. Vulnerability Rating: Architectural Vulnerabilities		
ID	Tunnel Characteristics	Attribute Options
4.1	**Number of Tubes** Number of distinct openings (circular or square) or bores that vehicles or trains pass through.  *c. Tunnel with more than two tubes*	a. 1 b. 2 c. More than 2
4.2	**Servics Entrance** Any entrance used by the transit organization's personnel that is not open to the general public and not used for emergency evacuation. 	a. **No.** No service entrance b. **Yes.** One or more service entrance(s)

4. Vulnerability Rating: Architectural Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
4.3	**Crowding/Congestion** Potential for traffic tie-ups in the tunnel.	a. Never crowded b. Sometimes c. Rush hour only d. Always crowded
4.4	**Emergency Exits** Emergency exits are egresses that facilitate the evacuation of riders and emergency personnel operations during an incident. Emergency exits should be clearly designated with the proper signage. The screener should count the number of independent (separate from public exits) emergency exits in the tunnel.  	a. More than 4 b. 3 to 4 c. 2 d. 1 e. None
4.5	**Number of Levels** Number of levels open to the public, including platforms, lobbies, concourses/mezzanines, fare control areas, transfer passageways, service, and other areas in the tunnel. For below-grade tunnels, the street level should not be considered unless the tunnel has features that make it an attractive target at this level.  *b. Two-level highway tunnel (courtesy, Washington State Department of Transportation)*	a. 1 b. 2 to 3 c. More than 3

4. Vulnerability Rating: Architectural Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
4.6	**Ease of Egress from Vehicle/Trains to Tunnel** Ability for an aggressor to exit the train or vehicle into the tunnel in non-emergency situations.	a. Difficult b. Moderate c. Easy
4.7	**Flood Gates** Adjustable gates used to control or stop water flow in a water surge.  *b. Floodgate on the right lining of a subway tunnel*	a. Yes b. No

4. Vulnerability Rating: Architectural Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
4.8	**Plaza/Public Areas** Open public space outside the controlled access to the tunnel. The plaza can be at grade or below grade and sometimes has public seating and seating areas. Plazas provide a pleasant space for people to relax, converse, and enjoy the outdoors in a more spacious setting; however, if not properly designed, plazas can leave the tunnel susceptible to an attack. Barriers and landscape features should be designed to make the plaza impenetrable to a vehicle. Furthermore, the plaza should be under surveillance using cameras and/or patrols.	a. **None**. No plaza/public area. b. **Well-controlled.** Public plaza has numerous barriers that are well-positioned to obstruct vehicular entry and surveillance is conducted. c. **Medium control.** Public plaza has some vehicular barriers but has several notable security flaws (e.g., temporary or ornamental barriers that can easily be defeated by vehicles). d. **Not controlled.** Public plaza has no vehicular barriers or surveillance.



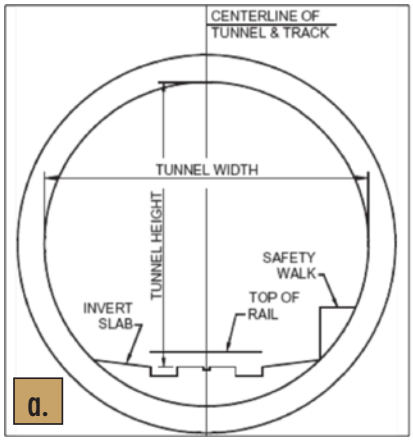
b. Below-grade public plaza leading to a transit entrance with numerous obstacles between traffic and the transit entrance

c. Public plaza with some protection.

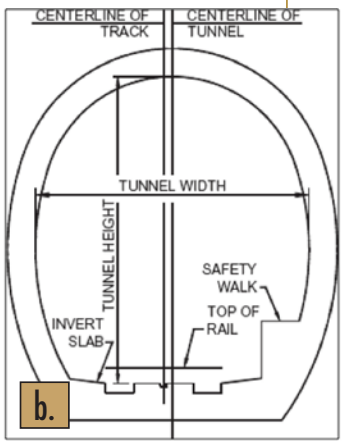
d. Public area adjacent to a subway station without limited-access management controls

Table 4-3c: Catalog of Tunnel Characteristics and Attribute Options for Structural Vulnerabilities

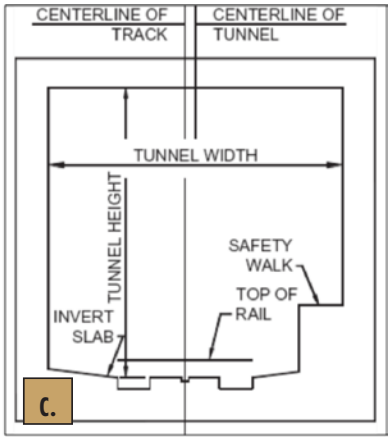
5. Vulnerability Rating: Structural Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
5.1	**Method of Construction** Technique used to build the tunnel.	a. **Drilled rock.** Built through rock. b. **Drilled soil.** Built through dirt or other soft materials such as sand. c. **Cut-cover.** Built by uncovering the street or ground, building the necessary tunnel shells, and rebuilding the area above d. **Immersed.** Assembled in large sections, moved to the proper area, and assembled with other sections onsite.
5.2	**Liner Cross Section** Shape of a tunnel from the onlooker's view.	a. Circular b. Oval c. Rectangular/square



a. Circular liner cross section (FHWA, 2005)



b. Oval liner cross section (FHWA, 2005)



c. Single box liner cross section (FHWA, 2005)

5. Vulnerability Rating: Structural Vulnerabilities

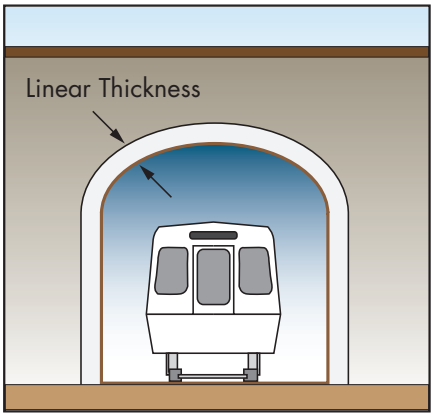
5.3 Liner Relative Thickness

Liner (or roof/wall) relative thickness refers to the thickness of the structural roof, wall, or envelope outlining the tunnel. A tunnel that has a thin liner that spans a long distance tends to be more vulnerable than one with a thicker liner and shorter span. In general, the relative liner thickness can be found in structural drawings of the tunnel. Such information is difficult to ascertain visually, especially by the nonprofessional screener. For an approximate evaluation of this characteristic, the construction material of the liner can provide some clues to the relative liner thickness. The table below provides general guidelines for relationships between construction materials and relative liner thickness.

Construction Material/Visible Structural Details	Relative Liner Thickness
Non-Reinforced Masonry	Thick
Reinforced Masonry	Thick
Other types of brick, stone, or rock based materials	Thick
Non-Reinforced Concrete	Thick
Reinforced Concrete	Medium
Iron (usually non-ductile older construction)	Thin Note: Watch for stiffeners (ribs); if not closely spaced or not visible, categorize as 'medium'
Steel	Thin (older construction) Very thin (newer construction)
Pre-stressed/post-tensioned concrete	Thin
High strength concrete	Thin
High strength steel	Very thin

Attribute Options

a. Not applicable. Station is above grade
b. Thick
c. Medium
d. Thin
e. Very thin



Linear thickness

b. Relatively think stone liner

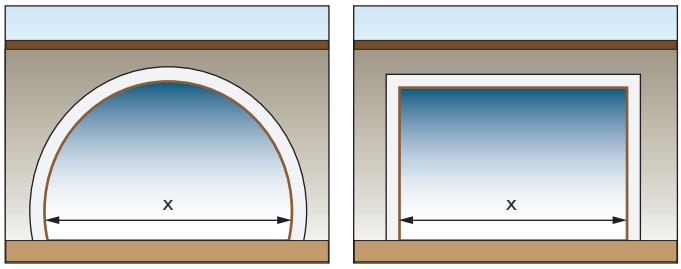
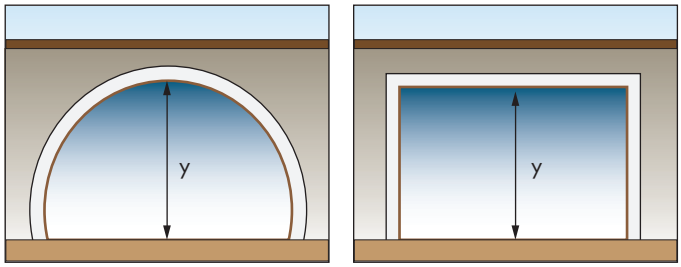
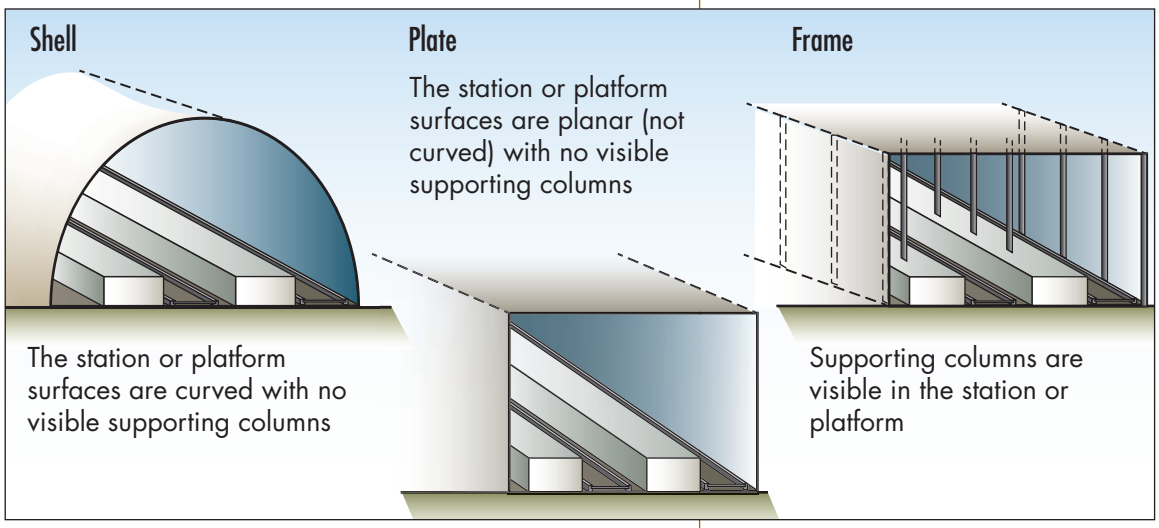
5.4 Construction Material

Primary material used to construct the tunnel's structural framework and envelope.

Attribute Options

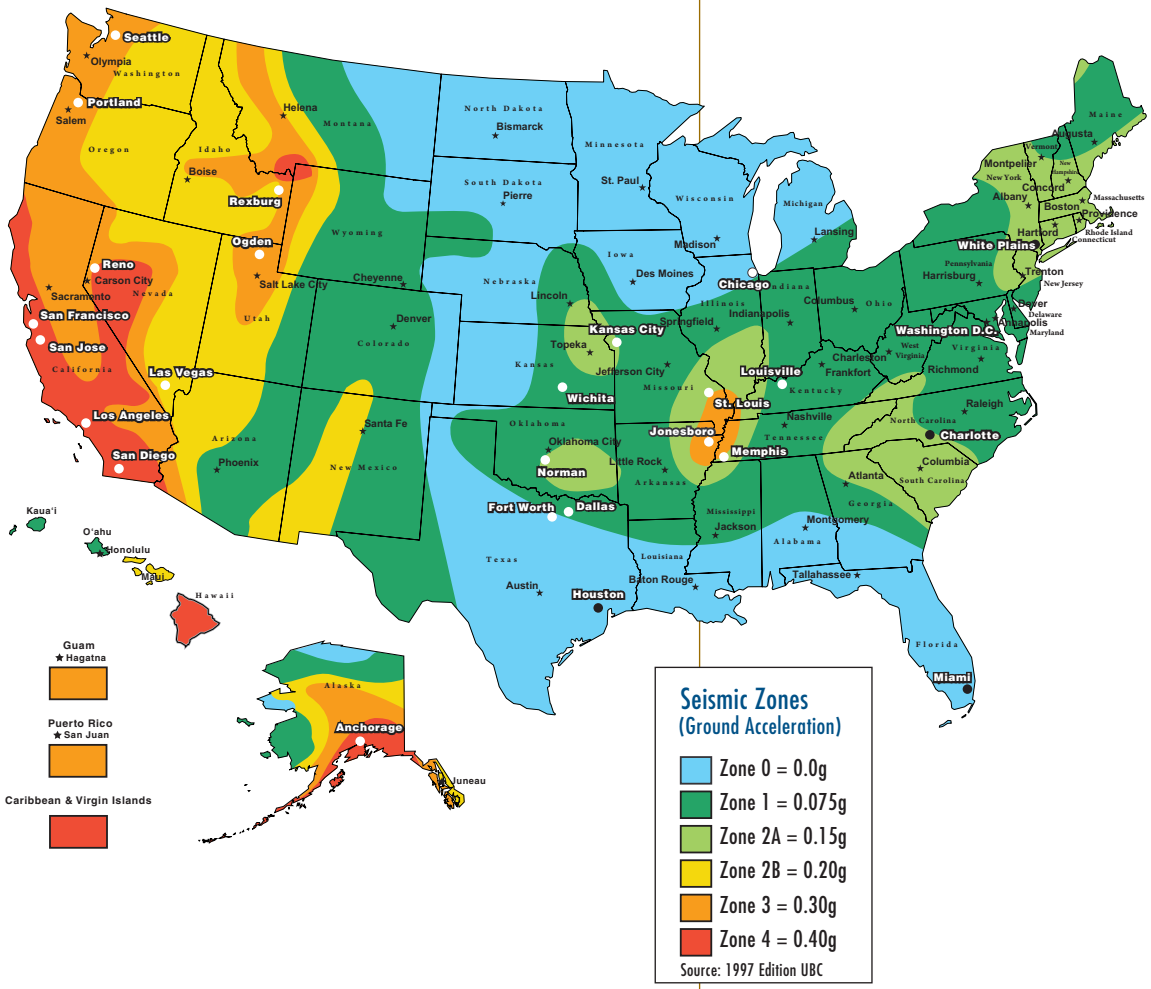
a. **High-strength concrete or steel.** Modern high-strength material is found primarily in recent retrofits and new construction and is extremely strong and blast-resistant.
b. **Steel/concrete/pre-stressed concrete**
c. **Wrought iron**
d. **Brick or masonry.** Brick, stone, and cinderblock materials used as the primary means of construction

5. Vulnerability Rating: Structural Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
5.4	**Construction Material (continued)**  b. Steel/concrete/pre-stressed concrete	 *c. Wrought iron*  *d. Brick or masonry*
5.5	**Known Retrofits** Recent structural upgrades to the tunnel including any addition of new technology or features to the existing system to increase the strength, durability, and/or service life of the structure.	a. Yes b. No
5.6	**Longest Span** Greatest distance between columns or other supporting structures.	a. Not Applicable b. 15 to 25 feet c. 25 to 40 feet d. 40 to 50 feet e. 50 feet or more

5. Vulnerability Rating: Structural Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
5.6	**Longest Span (continued)**  *Cross section illustrating the span of a circular tunnel* *Cross section illustrating the span of a Rectangular tunnel*	
5.7	*Controlliing Height* Average distance from floor to roof or ceiling.  *Cross section illustrating the height of a circular tunnel* *Cross section illustrating the height of a Rectangular tunnel*	a. Not applicable b. Less than 25 feet c. 25 to 40 feet d. 40 to 50 feet e. 50 feet or more
5.8	**Type of Framing** Type of structural frame or "skeleton" to which the interior and exterior envelopes of the tunnel are attached.  *Shell, plate, and frame framing*	a. Shell b. Plate c. Frame

5. Vulnerability Rating: Structural Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
5.7	**Seismic Design** Stations in active fault/earthquake zones that were built with or retrofitted with seismic design to be resistant to earthquakes.	a. **Not applicable.** Not in a high seismic zone and does not require seismic design b. **Yes.** In an seismic zone and incorporates seismic design c. **No.** In an seismic zone and does not incorporate seismic design elements

United States Seismic Zones Map



5. Vulnerability Rating: Structural Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
5.8	**Overall Structural Condition** State of tunnle maintenance, basic upkeep, and relative deterioration of important structural elements. Indicators of poor structural condition include aging members, discoloration, cracks, deflection, excessive vibrations, spalled or delaminated concrete, and corrosion. New materials, retrofitting, and lack of visual flaws may be taken as a sign of healthy structural condition	a. **Excellent.** Recently built or retrofitted. b. **Good.** Well maintained with few structural flaws. c. **Average.** A few major structural flaws, but none of them will impede safe transit operations or pedestrian movement. d. **Below average.** Major flaws in critical structural components that have the potential, without proper maintenance/repair, of impeding transit operations or pedestrian movement. e. **Poor.** Nearly unusable from lack of maintenance or other problems that have caused structural deterioration.

Table 4-3d: Catalog of Tunnel Characteristics and Attribute Options for Ventilation Vulnerabilities

6. Vulnerability Rating: Ventilation Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
6.1	**Protection of Ventilation Shafts** Degree of protection and security features of the tunnel's ventilation shafts. Ventilation shafts are typically small openings in the ground that permit air intake or exhaust and rarely have significant above-ground structural components (for larger structures, see ID 6.2).  *c. Vent shaft partly protected from traffic and pedestrians behind a wall and fencing.*	a. **Not applicable** b. **Well-protected.** Vent is well shielded or is not visible to passers-by c. **Somewhat protected.** Vent has limited protection but is still vulnerable. d. **Not protected.** Vent is completely exposed; no attempt has been made to shield the vent from any hazard  *d. Ventilation shaft exposed at the street level with no protection*

6. Vulnerability Rating: Ventilation Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
6.2	**Protection of Ventilation Structures** The degree to which major vent structures are shielded from vehicular attacks, accidents, or natural events. Certain tunnels (mainly vehicular tunnels) require ventilation buildings to provide the tunnel with essential ventilation.	a. **Not applicable** b. **Well-protected.** Protected from failure in the event of an attack, accident, or natural disaster c. **Somewhat protected**. Has features, either manmade or natural, so that it is shielded but not completely protected from an attack, accident, or natural disaster d. **Not protected.** No standoff distance from vehicles or exposed to natural hazards or another structural feature could cause ventilation functions to be compromised

b. Vent building protected from maritime attack by fencing, standoff, and a manned guard booth

c. Vent tower with partial protection from jersey barriers but little standoff distance

b. Vent buildings protected from vehicular impact by a double row of trees and decorative masonary and iron structures

d. Vent structure clearly labeled and without any barriers protecting it from vehicular impact

6. Vulnerability Rating: Ventilation Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
6.3	**Redundancy of Ventilation Systems** Reliability of the ventilation system if one or more components of the tunnel's system fail. Redundant ventilation systems provide an alternative or fail-safe by allowing connection to a backup system.	a. Not applicable b. Yes c. No
6.4	**Ventilation Hardware Exposure** Degree to which ventilation systems are visible and accessible to the general public.  *b. Hardened enclosure*	a. **Not applicable** b. **Hardened enclosure.** HVAC system is behind secured doors and vents where it is neither visible nor accessible to the general public. c. **Covered, not hardened.** HVAC system is not visible to the general public but is accessible through unsecured doors, vents, or other access points. d. **Visible.** HVAC system is exposed and unprotected.

Table 4-3e: Catalog of Tunnel Characteristics and Attribute Options for Fire Protection System Vulnerabilities

7. Vulnerability Rating: Fire Systems Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
7.1	**Protection of Fire Control Equipment** Fire extinguishers, hoses, and other fire control equipment should be kept in a secure enclosure that allows them to be accessed in case of emergency.  *a. Fire control panel in a locked enclosure.*	a. Yes b. No

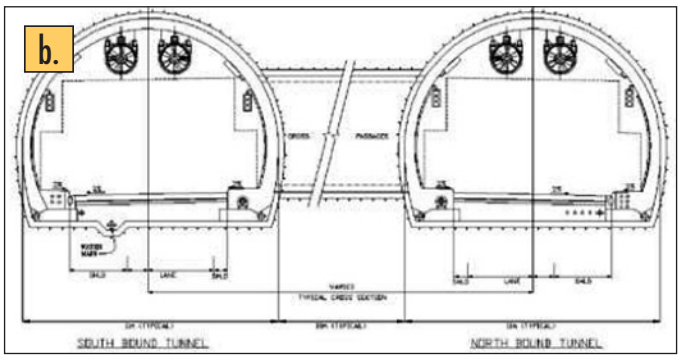
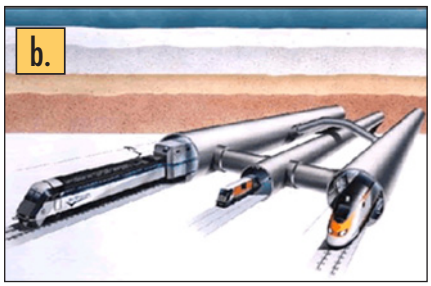
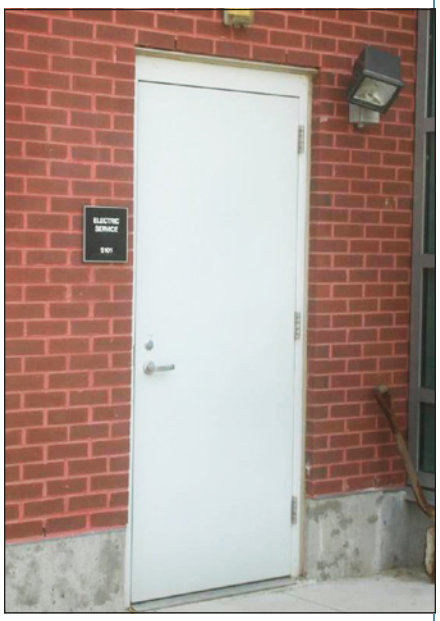
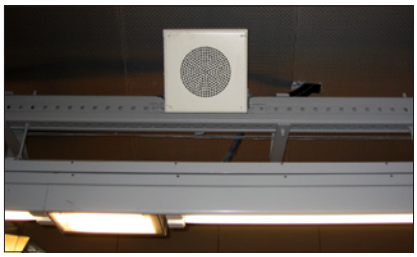
7. Vulnerability Rating: Fire Systems Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
7.2	**Effectiveness of Protection of Fire Control Equipment** Ability of enclosures to protect fire control equipment from unauthorized personnel and from other hazards.	a. Not applicable b. High c. Medium d. Low e. None
7.3	**First Responder Awareness of and Accessibility to Fire Equipment** First responder awareness of the location of the fire control equipment and whether this equipment is easily accessed.	a. Yes b. No
7.4	**Emergency Lighting** Illuminates the tunnel in a fire or other emergency situation or if the normal lighting system ceases to function. Emergency lighting includes having a clearly lit evacuation path and emergency exit signage.	a. Yes b. No
7.5	**Presence and Adequacy of Tunnel Cross Passageways** Cross passageways between parallel tunnels allow the movement of people from one tunnel to the other in an emergency. For example, if there is a fire in one tunnel, riders can be evacuated off the trains and through the cross passageway to the parallel  *b. A double tube tunnel with an adequate pedestrian cross passageway*	a. Single tube b. Double-tube adequate connector c. Double-tube not adequate  *b. Three tunnel tubes with a pedestrian cross passageway between all three*

Table 4-3f: Catalog of Tunnel Characteristics and Attribute Options for Operations Vulnerabilities

8. Vulnerability Rating: Operations Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
8.1	**Power Supply and Distribution: Enclosures** Enclosures of power supplies include any covering of electrical equipment, generators, and other supporting infrastructure necessary for facility operations.  *a. Secure entrance to a power supply area with a hardened door and electronic key pad entry*  *c. Power supply system, with only a chain link fence for protection, exposed to the public and subject to tampering*	a. **Well protected.** Power supplies are behind hardened enclosures with secure access points. b. **Marginally protected.** Power supply systems are concealed but not sufficiently hardened to withstand intentional tampering or a natural disaster. c. **Not protected.** Power supplies are exposed and easily accessible to the general public.  *b. Power supply system behind a non-hardened door with a traditional lock and key entry system*

8. Vulnerability Rating: Operations Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
8.2	**Surveillance and Control**	
8.2.1	**Coverage of Control Systems** The number of surveillance, intrusion detection, and access management/control systems in operation describes the total number of security systems in place that are designed to allow facility personnel to monitor public behavior. Security systems can be simple or as complex as a comprehensive integrated intrusion detection system that includes a closed circuit television (CCTV) network.  *Two security systems, a CCTV camera and a mirror, are each different types of surveillance systems with differing qualities and deterrence values*	a. **Complete.** The traveling public is under surveillance from the time they enter the station until the time they board the train. b. **Partial.** The traveling public is under surveillance from the station entrance through fare collection area, or from the collection area to the platform. c. **None.** There are no control systems in operation to cover the traveling public from the time they enter the station until they board the train.
8.2.2	**Quality of Control Systems** Describe the operational quality of surveillance and control systems in operation based on the age of the equipment. The screener should note the age of the equipment in the Comments column.	a. **High** b. **Medium** c. **Low**

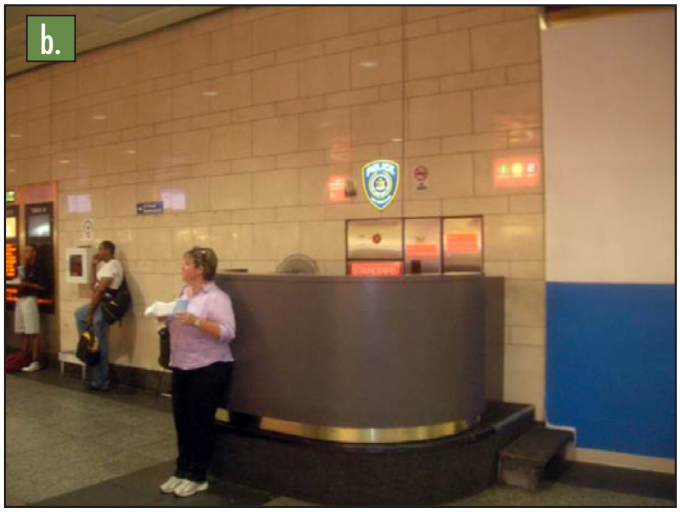
8. Vulnerability Rating: Operations Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
8.3	**Public Address and Communication:**	
8.3.1	**Public Notification (Alerts and Signage for Public Awareness)** Efforts by the transit agency to implement focused public awareness campaigns for transit agency employees and the traveling public, placing emphasis on public security and emergency awareness. Public awareness programs consist of security and emergency preparedness information materials prominently displayed throughout the system by signage, notifications, alerts, and public announcements. Attribute options are divided into small tunnels and large tunnels There are a total of 10 options for this characteristic. Only one attribute option should be selected. **Classification of Public Awareness** **Class 1.** Public awareness is a limited effort consisting of: • Signage • Posters • Public telephones. **Class 2.** Public awareness is a heightened effort. In addition to Class 1, Class 2 public awareness consists of: • Panic alarms (one-way communication) • Audible alerts through public address systems **Class 3.** The transit system has a dedicated public awareness campaign. In addition to Class 1 and Class 2, Class 3 public awareness consists of: • Real-time updates • Visual alert system • Emergency call boxes with two-way communication  *Electronic message board*	**Small tunnels** a. Class 3 b. Class 2 c. Class 1 d. Present (non-operational) e. None **Large tunnels** f. Class 3 g. Class 2 h. Class 1 i. Present (non-operational) j. None  *Audible public address system*  *Emergency aall box*
8.3.2	**Effectiveness of Public Awareness** Ability and success of the public awareness program to accomplish the following (through public notification, alerts, and signage): • Declare a state of an emergency • Urge passengers to report unattended property, suspicious behavior, and security concerns • Display security awareness and emergency preparedness information • Inform passengers of the means to evacuate safely from transit vehicles and/or facilities • Designate restricted areas All signage should be prominently displayed and legible to the public. Public address systems should be audible.	a. High b. Moderate c. Limited

8. Vulnerability Rating: Operations Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
8.3.3	**Asset-Related Communications** Systems available at the tunnel to facilitate rapid information gathering, decision-making, and response (action taking). Classification of Communications Systems: **Class 1.** Basic interdiction-related communications system that alerts the public to potential threats and provides a means for the public and staff personnel to report suspicious activity. Communications consist of: • Hand-held radios • Emergency notification alarm • Cell phones • Telephones **Class 2.** Enhanced interdiction-related communications system that provides appropriate modes of communication capabilities to security, staff personnel, and public. In addition to Class 1, Class 2 communications consists of: • Multi-channeled hand-held radios • GPS • Pagers **Class 3.** Optimal interdiction-related communications system that provides secure, interoperable, and redundant modes of communication capabilities to security, staff personnel, and appropriate communications for the public. In addition to Class 1 and Class 2, Class 3 communications consist of: • Secure communications with multiple channels, frequencies, and additional means should primary means fail • Communications channeled through a dedicated proprietary communications center	**Small tunnels** a. Class 3 b. Class 2 c. Class 1 d. Present (non-operational) e. None **Large tunnels** f. Class 3 g. Class 2 h. Class 1 i. Present (non-operational) j. None
8.3.4	**Effectiveness of Asset-Related Communications** Ability and success of the asset-related communications to accomplish the following through hand-held radio, emergency alarms, telephones, and emergency callback boxes: • Facilitate rapid information gathering • Facilitate decision-making • Facilitate response and action taking	a. High b. Moderate c. Limited

8. Vulnerability Rating: Operations Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
8.4	**Quality of Lighting** Lighting in tunnels is crucial for motorists and train operators. It has both safety and security purposes. In conjunction with the lighting system, a highly reflective surface on the walls and ceiling, such as tile or metal panels, may be used.	
8.4.1	**Effectiveness of Exterior Lighting** The effectiveness of illumination at the approaches to the tunnel. Security lighting should be provided for the overall site to allow security personnel to maintain visual assessment during hours of darkness. Continuous or periodic observation may provide both a real and psychological deterrent because it facilitates detection of unauthorized personnel and makes the job of an attacker more difficult.	a. **High.** Approaches are well lit, and lighting is well maintained. b. **Medium.** Tunnel approaches have areas where lighting should be improved or where lighting is not well maintained. c. **Low.** Tunnel exterior lighting is ineffectual or nonexistent.
8.4.2	**Sufficiency of Interior Lighting** Sufficiency of illumination inside the main functioning areas of the tunnel.  *a. Tunnel with effective interior lighting*	a. **High.** Lighting for standard operations, such as regular vehicular movement, is sufficient. b. **Medium.** Lighting systems either need replacement, basic maintenance, or minor upgrades. c. **Low.** Facility lighting systems are either nonexistent or of such poor quality that the facility interior is barely passable and other sources of light, such as flashlights, are needed to operate in the tunnel.

Table 4-3g: Catalog of Tunnel Characteristics and Attribute Options for Nonstructural Vulnerabilities

9. Vulnerability Rating: Nonstructural Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
9.1	**Wall and Ceiling Finish** Coverings that are attached to the structural framing and are not intended or designed to resist loads but are important to the overall tunnel function. finishes can provide the following: • Enhanced tunnel lighting • Fire resistance • Noise attenuation • Aesthetics Finishes include: • Ceramic tiles • Porcelain-enameled metal panels • Epoxy-coated concrete • Coated cemented-board panels • Precast concrete panels • Metal tiles	a. **High.** Well-maintained and securely attached to the structure. There have been no recent reports or signs of falling debris from the wall or ceiling. b. **Medium.** Need basic maintenance, parts have recently fallen, and/or there are some missing sections. Issues with wall and/or ceiling finishes have not significantly affected tunnel operations. c. **Low.** Finishes have caused operational issues in the tunnel; there is a significant backlog of maintenance, and/or there are large mission sections of tile on walls.
9.2	**Pavement Driving/Track Quality** Overall condition and defects of the pavement or rail tracks in the tunnel.	a. **High.** Few if any potholes and other obstructions and in a good state of repair. b. **Medium.** Some potholes and other obstructions and needs some repair. Overall the tunnel is passable. c. **Low.** Full of potholes and/or other obstacles, making passage nearly impossible
9.3	**Quality of Security Personnel Booths** Provide information on the existence and rating for any law enforcement installations inside or immediately adjacent to the tunnel that act to directly support public safety in the facility.  *a. Example of high-quality modern security personnel booth facility*	a. **High.** Modern facility with command and control equipment, intrusion detection, access management controls, permanent structural components, and other features that enable public safety officials to monitor the station complex. b. **Medium.** Police booths without significant surveillance capabilities and little or no major structural components. c. **Low.** Temporary or poorly made structure without station surveillance equipment. d. **None**

9. Vulnerability Rating: Nonstructural Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
9.3	**Quality of Security Personnel Booths (continued)**  *b. Example of medium-quality security personnel booth*	 *c. Example of low-quality security personnel booth*
9.4	**Fixture Attachments** Lighting, wiring, piping, and other exposed components.  *a. Example of secure fixture attachments.*	a. **Secured.** Fixture attachments are secure from accidental incidents, vandalism, and other acts that might disrupt operations. b. **Not secured.** Fixture attachments are exposed to accidental events, vandalism, or other acts that might cause a disruption of service.  *b. Example of fixture attachments that are not secure*

9. Vulnerability Rating: Nonstructural Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
9.5	**Quality of Barriers/Curbs** Existence and effectiveness of barriers and curbs in preventing vehicles from damaging the tunnel complex.	a. **High.** Existing barriers or curbs are of good quality and sufficient to stop a vehicle from entering the station. b. **Medium.** Existing barriers or curbs are sufficient to stop an accidental impact at the station but would not stop an intentional vehicular attack at the station. c. **Low.** Barriers or curbs would not stop even an accidental vehicular impact at the station. d. **None present**

Table 4-3h: Catalog of Security Systems for Physical Security Vulnerabilities

10a. Vulnerability Rating: Physical Security Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
10.1a	**Access Control** Any combination of equipment and/or guards that can deny entry to unauthorized personnel or vehicles to certain areas of the tunnel. The function of access control is to ensure that only authorized personnel are permitted into or out of a controlled area. Entry can be controlled by locked fence gates, locked doors to a building or rooms in a building, or specially designed portals. The means can be applied manually by guards or automatically by using entry control devices . Examples of access control systems: • Fare collection gates • Electronic keypad • Magnetic-stripe card • Proximity card • Smart card • Biometric devices	a. Yes b. No

10a. Vulnerability Rating: Physical Security Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
10.2a	**Intrusion Detection Systems (IDS)** The combination of components, including sensors, control units, transmission lines, and monitor units, integrated to operate in a specific manner. The purpose is to detect an aggressor crossing the boundary of a protected area. The sensors initiate alarm signals by sensing the stimulus, change, or condition for which it was designed. Examples of exterior intrusion detection sensors: • Fence • Buried line • Microwave • Infrared Examples of interior intrusion detection sensors: • Boundary penetration • Volumetric motion • Video analytics	a. Yes b. No
10.3a	**Video and Surveillance Assessment – Monitored CCTV** An electronic system of cameras, control equipment, recorders, and related apparatus used for surveillance or alarm assessment. The system may include event-activated software. Effectiveness of the system depends on proper monitoring, the resolution, and coverage of the cameras.	a. Yes b. No
10.4a	**Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE) Detection Equipment** A variety of technologies and techniques that are in a fixed location to detect the presence or use of CBRNE weapons in real-time. Examples of CBRNE detection equipment: • Trace detection equipment • Vapor sampling • CBR identifiers and classifiers • Integrated system	a. Yes b. No  *Fixed CBR identifier*
10.5a	**Personnel/Baggage CBRNE Screening** Search and screening are conducted at a fixed check point. Anomalies are verified with K-9 and other CBRNE detection devices.	a. Yes b. No

10a. Vulnerability Rating: Physical Security Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
10.6a	**Vehicular CBRNE Screening** Vehicles are searched and screened at fixed checkpoints. Anomalies are verified with K-9 and other CBRNE detection devices.	a. Yes b. No
10.7a	**Mobile Personnel/Baggage CBRNE Screening** Random searches are conducted of personnel and baggage, typically by a roving team of personnel with appropriate equipment and an explosive K-9 Unit.	a. Yes b. No
10.8a	**Unarmed Guards/Patrol** Security guards at the tunnel carry no firearms and are responsible for detecting, deterring, observing, and reporting malicious behavior.	a. Yes b. No
10.9a	**Armed Guards/Patrols** Security guards patrolling at the tunnel are armed and meet all appropriate jurisdiction standards. The guard/patrol is responsible for reporting incidents and has a limited interdiction capability.	a. Yes b. No
10.10a	**Law Enforcement Patrols (Landside)** Sworn law enforcement personnel patrol during specified hours or randomly patrol the tunnel.	a. Yes b. No
10.11a	**Asset/Interdiction-related Communications** Security communication systems that facilitate rapid information gathering, decision-making, and actions (response). Examples: • Pagers • GPS • Multi-channeled hand-held radios • Two-way radio • Direct ring-down intercoms • Standard telephone landlines • Wireless phones • Emergency notification alarm	a. Yes b. No

10a. Vulnerability Rating: Physical Security Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
10.12	**Special Weapons and Tactics (SWAT) Teams** A special tactical unit trained for multiple special operations that is either full-time to the transit system or provided by the local law enforcement. The SWAT team is trained in counterterrorism and possesses specialized skills in explosive breaching, sharpshooter capability, hostage rescue, etc.	a. Yes b. No
10.13	**10.13 Explosion ordinance disposal (EDO) teams** A special team either full-time dedicated to the transit system or provided by the local law enforcement who are trained to be used as a bomb squad when needed.	a. Yes b. No

10b. Vulnerability Rating: Waterside Security Systems (Applicable to Underwater Tunnels)		
ID	**Tunnel Characteristics**	**Attribute Options**
10.1b	**Number of Systems** Number of security systems available to protect against the threat of an explosion inside the subway station. This characteristic is automatically summed in the IRVS Database using the general security system checklist.	a. Yes b. No
10.2b.	Vessel Boarding Teams Team with the ability to board vessels near the tunnel in security or emergency situations .	a. Yes b. No
10.3b	**Dive Teams** Team with the capability to dive into the water surrounding the tunnel for security purposes.	a. Yes b. No
10.4b	**Patrol Boats** Vessels used for emergency response at the tunnel	a. Yes b. No

10c. Vulnerability Rating: Physical Security Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
10.1c	**Blast Threat: Internal** Intrusion into the transit tunnel by a person or persons with the intent to attack the transit tunnel with an explosive device.	
10.1.1c	**Number of Systems** Number of security systems available to protect against the threat of an explosion inside the subway tunnel. This characteristic is automatically summed in the IRVS Database using the general security system checklist.	a. 8 or more b. 4 to 7 c. 1 to 3 d. None

10c. Vulnerability Rating: Physical Security Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
10.1.2c	**Overall Security Effectiveness** Ability and success of the collective security systems to protect against the threat of an explosion inside the transit tunnel. The number of detection systems available will have little impact if the systems are not effective in thwarting attacks.	a. High b. Effective c. Minimal d. Ineffective e. No security
10.2c	**Blast Threat: External (Direct)** Use of an explosive device to attack the transit tunnel from the exterior. In this case, the transit tunnel is the primary target.	
10.2.1c	**Number of Systems** Number of security systems available to protect against an explosion outside the transit tunnel. This characteristic is automatically summed in the IRVS Database using the general security system checklist.	a. 5 or more b. 3 to 4 c. 1 to 2 d. None
10.2.2c	**Overall Security Effectiveness** Ability and success of the collective security systems to protect against the threat of an explosion directed at the transit tunnel from the exterior. The number of detection systems available will have little impact if the systems are not effective in thwarting attacks.	a. High b. Effective c. Minimal d. Ineffective e. No security
10.3c	**Blast Threat: External (Collateral)** An attack with explosive devices on a target within a 300-foot radius of the transit tunnel e.g., a bomb explosion in a plaza adjacent to a transit tunnel.. The transit tunnel is not the primary target but would be susceptible to collateral effects.	
10.3.1c	**Number of Systems** Number of security systems available to detect the threat of an explosive attack on a target within 300-feet of the transit tunnel. The tunnel is not the primary target but would be susceptible to collateral effects. The detection systems may be separate from security operations of the tunnel. Redundant systems are highly desirable. This characteristic is automatically summed in the IRVS Database using the general security system checklist.	a. 5 or more b. 3 to 4 c. 1 to 2 d. None
10.3.2c	**Overall Security Effectiveness** Ability and success of collective security systems to protect the transit tunnel against the collateral effects of an explosive attack on another target within 300 feet. The number of detection systems available will have little effect if the systems are not effective in thwarting attacks.	a. High b. Effective c. Minimal d. Ineffective e. No security

10c. Vulnerability Rating: Physical Security Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
10.4c	**CBR Threat: Tunnel** The release of a CBR agent inside the tunnel.	
10.4.1c	**Number of Systems** Number of security systems available to detect the threat of a CBR release inside the tunnel. Detection systems include access control, screening systems, sensors, video surveillance and assessment, security lighting, and security guards. Redundant systems are desirable. This characteristic is automatically summed in the IRVS Database using the general security system checklist.	a. 5 or more b. 3 to 4 c. 1 to 2 d. None
10.4.2c	**Overall Security Effectiveness** Ability and success of the collective security systems to protect against the threat of a CBR release inside the tunnel. The number of detection systems available will have little effect if the systems are not effective in thwarting attacks.	a. High b. Effective c. Minimal d. Ineffective e. No security
10.5c	**CBR Threat: External** The release of a CBR agent outside the tunnel.	
10.5.1c	**Number of Systems** Number of systems available detect the threat of a CBR release inside the tunnel of the tunnel. Detection systems include access control, screening systems, sensors, video surveillance and assessment, security lighting, and security guards. Redundant systems are highly desirable. This characteristic is automatically summed in the IRVS Database using the general security system checklist.	a. 5 or more b. 3 to 4 c. 1 to 2 d. None
10.5.2c	**Overall Security Effectiveness** Ability and success of the collective security systems to protect against the threat of a CBR release inside the tunnel of the tunnel. The number of detection systems available will have little effect if the systems are not effective in thwarting attacks.	a. High b. Effective c. Minimal d. Ineffective e. No security
10.6	**Fire Threat: Internal** Fire threat inside the tunnel that threatens the life safety of vehicular passengers and riders and the operations of the tunnel itself.	
10.6.1c	**Number of Systems** Number of detection systems available for security purposes that can also serve as protection against the threat of a fire inside the tunnel This characteristic is automatically summed in the IRVS Database using the general security system checklist.	a. 5 or more b. 3 to 4 c. 1 to 2 d. None
10.6.2c	**Overall Security Effectiveness** Ability and success of the collective security systems to protect the tunnel against the threat of a CBR release outside the transit tunnel. The number of detection systems available will have little effect if the systems are not effective in thwarting attacks.	a. High b. Effective c. Minimal d. Ineffective e. No security

10c. Vulnerability Rating: Physical Security Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
10.7c	**Fire Threat: Tunnel/Track/Smoke** Fire or smoke in the tube of the tunnel that threatens life safety, operations, and structure of the tunnel.	
10.7.1c	**Number of Systems** Number of security systems available for security purposes that can also serve as protection against the threat of a smoke inside the tunnel. This characteristic is automatically summed in the IRVS Database using the general security system checklist.	a. 5 or more b. 3 to 4 c. 1 to 2 d. None
10.7.2c	**Overall Security Effectiveness** Ability and success of the collective security systems to protect (detect and interdict) against the threat of a smoke inside the tunnel. The number of detection systems available will have little impact if the systems are not effective in thwarting attacks.	a. High b. Effective c. Minimal d. Ineffective e. No security
10.8c	**Other Threats: Flood/Flooding** Event causing the tunnel to be submerged in water, threatening the operations and users of the tunnel.	
10.8.1c	**Number of Systems** Number of detection systems available to protect against the threat flooding in the tunnel. This characteristic is automatically summed in the IRVS Database using the general security system checklist.	a. 5 or more b. 3 to 4 c. 1 to 2 d. None
10.8.2c	**Overall Security Effectiveness** Ability and success of the collective security systems to protect (detect and interdict) against the threat of a flood inside the tunnel. The number of detection systems available will have little impact if the systems are not effective in thwarting attacks.	a. High b. Effective c. Minimal d. Ineffective e. No security
10.9c	**Other Threats: Cyber** An attack on the transit tunnel through any combination of facilities, equipment, personnel, procedures, and communications integrated through cyber networks or control systems.	
10.12.1c	**Number of Systems** Number of detection systems available to protect against the threat of a cyber attack on the tunnel. This characteristic is automatically summed in the IRVS Database using the general security system checklist.	a. 5 or more b. 3 to 4 c. 1 to 2 d. None
10.12.2c	**Overall Security Effectiveness** Ability and success of the collective security systems to protect the tunnel against the threat of a cyber attack on the tunnel. The number of detection systems available will have little effect if the systems are not effective in thwarting attacks.	a. High b. Effective c. Minimal d. Ineffective e. No security

Table 4-3i: Catalog of Tunnel Characteristics and Attribute Options for Cyber Vulnerabilities

11. Vulnerability Rating: Cyber Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
11.1	**Effectiveness of Cyber Security Plan** How well the security in place to protect systems, such as the supervisory control and data acquisition (SCADA) or utility monitoring and control systems (UMCS), which provide monitoring and control of utilities within buildings or the electronic security system. Many tunnel operation systems use the Internet to perform these functions, so cyber security must be a priority because the systems are accessible to all attackers with a computer and access to the Internet. The best protection for these systems is to remove them from the Internet; when that is not feasible, other protective features must be put in place.	a. High b. Medium c. Low d. None
11.2	**Effectiveness of Training Programs** Effectiveness of the programs in place to train transit tunnel employees on the cyber security measures in place.	a. High b. Medium c. Low d. None
11.3	**Security of Communication, Signal, and Power Systems** Measures in place to protect the communication system, signal system, and power supply to the tunnel.	a. Secured b. Medium c. Marginal d. No security
11.4	**Redundancy of Communication Systems** The tunnel's ability to operate communications systems if the primary system is compromised.	a. Yes b. No
11.5	**Security of Power Supply** Measures in place to protect the power supply to the tunnel. The power supply ensures that all communications and security measures are functioning.	a. Secured b. Medium c. Marginal d. No security
11.6	**Effectiveness of Wireless, Radio, or Satellite Systems During Emergencies** Whether these communication modes can function effectively to deliver important messages to the tunnel if other systems are compromised.	a. High (regional) b. Medium (within jurisdiction) c. Low (system only)

Table 4-3j: Catalog of Tunnel Characteristics and Attribute Options for Operational Security Vulnerabilities

12. Vulnerability Rating: Operational Security Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
12.1	**Emergency Plan** Emergency plans are procedures and protocols the transit agency is prepared to use when a disaster occurs. The purpose of emergency plans is to reduce the impact of disasters before, during, and after the threat. By implementing the emergency plan, a transit agency can enhance its capability to respond and recover and to mitigate against an act of terrorism or natural disaster.	a. Yes b. No
12.2	**Emergency Response Exercises** A well-rehearsed emergency plan enables efficient coordination of rescue and response operations. Drills and training can improve how people function during emergencies.	a. Full scale b. Table top c. Workshop d. None
12.3	**Effectiveness of Emergency Plans** Ability and success of the emergency/security response plans implemented by the tunnel. Just having a plan does not protect the tunnel; if the plan is not effective, the tunnel will not be prepared to respond to an emergency. Characteristics of an effective emergency/security response plan are: • Communication plans with easily understandable terminology and methods • Development and exercise of warnings combined with planned areas of refuge and evacuation plans • Development of organizations of trained volunteers among civilian populations such as, Community Emergency Response Teams	a. High b. Effective c. Minimal d. Ineffective
12.4	**Security Plan** Plan for the protective system, continuity of operations, and other emergencies. The plan includes details on how a system or process will be handled and often include general plans for system redundancy, continuity of operations, Memoranda of Understanding for response force support, and notification requirements.	a. Yes b. No
12.5	**Security Plan Update Status** Length of time since security plans were last updated. Security plans should be reviewed and updated annually to incorporate changes in threat intelligence.	a. Within 12 months b. 1 to 2 years c. 2 to 5 years d. More than 5 years e. None

12. Vulnerability Rating: Operational Security Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
12.6	**Transit Agency Mass Evacuation Plan** Procedure for immediately and rapidly move people out of the tunnel because of a threat or hazard. Mass evacuation plans are developed to ensure the safest and most efficient evacuation time for all of the people in the tunnel in the event of an emergency. The significance of having an evacuation plan depends on the size and expected use of the tunnel.	a. Both tunnel and train (if rail tunnel) b. Train only (if rail tunnel) c. None For vehicle tunnels, the answer will be either attribute option (a.) or (c.).
12.7	**Effective of Mass Evacuation Plan** Ability and success of the mass evacuation plan. An effective evacuation plan uses multiple exits and technologies to ensure full and complete evacuation. The transit agency should post procedures for safe evacuation prominently in the tunnel. The screener should consider the phases of evacuation when determining the effectiveness of the evacuation plan. 1. Detection 2. Decision 3. Alarm 4. Reaction 5. Movement to area of refuge or assembly tunnel 6. Transportation	a. High b. Effective c. Minimal d. Ineffective
12.8	**Continuity of Security** If security and protective measures are not maintained during off-peak or closing hours, the tunnel is more vulnerable.	a. Yes b. No
12.9	**Report/Exchange Threat Information** How often the transit agency receives and exchanges threat information with local, State, and Federal law enforcement officials.	a. Frequent b. Seldom/infrequent c. None

12. Vulnerability Rating: Operational Security Vulnerabilities		
ID	**Tunnel Characteristics**	**Attribute Options**
12.10	**Training Programs** Training and education for transit personnel (security, maintenance, and operations) is essential because it is the engagement and decision-making of these individuals, operating in their own areas of expertise and responsibility, that will determine the success of emergency preparedness and response. Training should be provided to all transit employees regarding security awareness and emergency response. Objectives for training are: • Develop employee awareness of potential threats or hazards. Employees should be able to recognize, report, and respond appropriately to suspicious items. • Develop an understanding of responses and protective actions and what to do for each of the possible emergency situations.	a. Well established b. Marginal c. None
12.11	**Coordinated Efforts of Local/Regional First Responders** Coordination of security and emergency management plans with local and regional first responders. A Mutual Aid Agreement should be established between the transit agency and entities in the area that would be called upon to supplement the agency's resources during an emergency. The collaboration should include: • Coordinated exercises with both entities for emergency preparedness and response • Sharing of emergency response and security protocols • Information sharing capabilities (e.g., contacts, procedures, resource inventories) • Interoperable communications systems with first responders (	a. Well established b. Marginal c. None

5

References

American Public Transit Association. 2011. *Public Transportation Ridership Report, Fourth Quarter 2010*. Available at http://www.apta.com/resources/ statistics/pages/ridershipreport.aspx. Accessed March 26, 2011.

DHS (Department of Homeland Security). 2002. *Transit Risk Assessment Module (TRAM)*.

DHS. 2007. "S&T Snapshots – Borders & Maritime; Find It and Plug It." Available at http://www.dhs.gov/files/programs/ gc_1217612281587.shtm. Accessed April 13, 2011.

DHS. 2009a. *Critical Infrastructure Resilience Final Report and Recommendations*. National Infrastructure Advisory Council.

DHS (Department of Homeland Security). 2009b. *National Infrastructure Protection Plan*. Department of Homeland Security, Washington, D.C.

DHS. 2011a. *Integrated Rapid Visual Screening of Buildings*.

DHS. 2011b. *Integrated Rapid Visual Screening of Tunnels*.

DHS. 2011c. *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, Building and Infrastructure Protection Series*, P 426. Science and Technology Directorate, Washington, D.C.

Encyclopædia Britannica. 2011. "Mass Transit." *Encyclopædia Britannica Online*. Available at http://www.britannica.com/EBchecked/topic/368374/mass-transit. Accessed April 26, 2011.

FEMA (Federal Emergency Management Agency). 2003. FEMA 426, *Reference Manual for the Protection of Buildings Against a Terrorist Attack*.

FEMA. 2005. FEMA 452, *Risk Assessment: A How To Guide to Mitigate Terrorist Attacks*. Risk Management Series.

FEMA. 2007. FEMA 430, *Site and Urban Design for Security*. Risk Management Series.

FEMA. 2009. FEMA 455, *Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks*. Risk Management Series.

FHWA (Federal Highway Administration). 2003. *Recommendations for Bridge and Tunnel Security*. Prepared by Blue Ribbon Panel on Bridge and Tunnel Security, Washington, D.C.

A

Acronyms

BIPS	Buildings and Infrastructure Protection Series
C	consequences
CBR	chemical, biological, and radiological
CBRNE	chemical, biological, radiological, nuclear, explosive
CCTV	closed circuit television
CIKR	Critical Infrastructure and Key Resources
DCF	Data Collection Form
DHS	Department of Homeland Security
EOD	explosive ordinance disposal teams
FEMA	Federal Emergency Management Agency
HSPD	Homeland Security Presidential Directorate
HVAC	heating, ventilation, and air conditioning

IDD	Infrastructure Protection and Disaster Management Division
IDS	intrusion detection system
IRVS	integrated rapid visual screening for mass transit stations
MBTA	Massachusetts Bay Transportation Authority
MS	Microsoft
MTS	mass transit station
NIPP	National Infrastructure Protection Plan
PANYNJ	Port Authority of New York & New Jersey
RMS	Risk Management Series
S&T	Science and Technology Directorate
SCADA	supervisory control and data acquisition
SWAT	special weapons and tactics teams
T	threat
TSA	Transportation Security Administration
UMCS	utility monitoring and control systems
V	vulnerabilities

B

Glossary

Access control. Any combination of barriers, gates, electronic security equipment, and/or guards that can deny entry to unauthorized personnel or vehicles.

Aggressor. Any person seeking to compromise a function or structure.

Assessment. The evaluation and interpretation of measurements and other information to provide a basis for decision-making.

Asset. Person, structure, facility, information, material, or process that has value.

Asset-related communications. Systems available to facilitate rapid information gathering, decision-making, and response (action taking).

Attack. Hostile action resulting in the destruction, injury, or death to the civilian population or damage or destruction to public and private property.

Attribute. Subcategory of characteristic. For example, station elevation is a characteristic, and a below-grade elevation is the attribute. Attributes are presented in the electronic software in a dropdown menu. In paper version of the data collection form, attribute options are presented in columns "a" to "e."

Biological agent. Living organisms or the materials derived from them that cause disease or harm to humans, animals, or plants or cause deterioration of material. Biological agents may be in liquid droplets, aerosols, or dry powders.

Business continuity. Ability of an organization to continue to function during and after a disaster.

Catalog. List of station characteristics and attributes that are assessed in the IRVS of mass transit stations. The catalog includes guidance on selecting attributes.

Catenary. System of overhead trolley wires that carry electric current, in which the contact wire is hung from another wire that hangs in a catenary curve; also, any or all of the overhead trolley wire system.

Characteristic. Physical component, functionality, or operation of a mass transit station that is evaluated in the IRVS procedure and listed on the Data Collection Form.

Chemical agent. Chemical substance that is intended to kill, seriously injure, or incapacitate people through physiological effects.

Closed circuit television. Electronic system of cameras, control equipment, recorders, and related apparatus used for surveillance or alarm assessment.

Collateral damage. Injury or damage to assets that are not the primary target of an attack.

Concourse. Open space that accommodates large crowds and allows for efficient distribution of people between locations.

Consequence. Effect of an event, incident, or occurrence. Consequences are divided into four categories: public health and safety, economic, psychological, and governance impacts.

Consequences rating. Degree of debilitation that would be caused by the incapacity or destruction of an asset.

Control center. Centrally located room or facility staffed by personnel charged with the oversight of specific situations and/or equipment.

Control system. Computer-based system used in many types of infrastructure and in many industries to monitor and control sensitive processes or physical functions.

Controlled area. Area into which access is controlled or limited; portion of a restricted area that is usually near or surrounding a limited or exclusion area.

Critical Infrastructure. Vital system or asset, either physical or virtual, that the incapacity or destruction of which may have a debilitating impact on the security, economy, public health or safety, environment, or any combination, across a Federal, State, regional, territorial, or local jurisdiction.

Cyber security. Protection that is intended to prevent damage to, unauthorized use of, or exploitation of, and if needed, restoration of electronic information and communications systems. Includes protection of information networks and wireline, wireless, satellite, public safety answering points, and communication and control systems.

Data Collection Form. Form containing the station characteristics and attribute options that is used in the IRVS of mass transit stations.

Deterrence. Inhibition of criminal behavior by fear especially of punishment.

Direct loss. Cost to rebuild, respond, and recover from an event.

Disaster. Natural catastrophe, technological accident, or human-caused event that results in severe property damage, deaths, and/or multiple injuries.

Downtime. Disruption of a service that is the result of an event, incident, or occurrence.

Emergency. Any natural or human-caused situation that results in or may result in substantial injury or harm to the population or substantial damage to or loss of property.

First responder. Local police, fire, and emergency medical personnel who arrive first on the scene of an incident and take action to save lives, protect property, and meet basic human needs.

Flood. Temporary, partial or complete inundation of normally dry land areas from overflow of inland or tidal waters, unusual or rapid

accumulation or runoff of surface waters, or mudslides/mudflows caused by accumulation of water.

Hazard. Natural or manmade source or cause of harm or difficulty.

Hazardous material. Any substance or material that, when involved in an accident and released in sufficient quantities, poses a risk to people's health, safety, and/or property. Includes explosives, radioactive materials, flammable liquids or solids, combustible liquids or solids, poisons, oxidizers, toxins, and corrosive materials.

Heavy rail. Electric railway with the capacity to handle a heavy volume of passengers.

Indirect loss. Downstream costs resulting from disruption of the service after an event.

Integrated rapid visual screening. Quick and simple procedure to assess the risk and resiliency of a mass transit station.

Intermodal. More than one mode of transportation (e.g., rail, bus, air).

Intrusion detection system. Combination of sensors, control units, transmission lines, and monitor units, integrated to operate in a specified manner.

IRVS Tier 1 assessment. Screening that identifies the primary facility vulnerabilities and.

IRVS Tier 2 assessment. Onsite evaluation by assessment specialists that provides a robust evaluation of system interdependencies, vulnerabilities, and mitigation options.

Key Resource. Publicly or privately controlled resource essential to the minimal operation of the economy and government.

Light rail. System characterized by vehicles that require an operator and are powered by overhead electric catenary or trolley wires. Often some portion of the route runs in the streets of cities or towns (as opposed to a heavy rail system in which vehicles operate on a private right-of-way). Modern equivalent of a trolley or interurban.

Liner. Roof/wall of underground stations or tunnels.

Liner relative thickness. Thickness of the structural roof/wall outlining an underground station to runnel.

Line. Transportation route that is typically distinguished by numbering, name, or color.

Lobby. Area with station attendants and fair collection machines.

Mass transit station. Structure acting as a terminal, typically underground or elevated, serving a mode of transportation for a mass transit system.

Mezzanine. Intermediate story in a station that projects in the form of a balcony.

Mitigation. Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident.

Natural protective barrier. Mountains, deserts, cliffs, ditches, water obstacles, or other terrain feature that is difficult to traverse.

Owner/operator. Entity responsible for day-to-day operation and investment in a particular asset or system.

Physical security. Measures/concepts designed to safeguard personnel; prevent unauthorized access to equipment, installations, material, and documents; and safeguard them against espionage, sabotage, damage, and theft.

Platform. Section of pathway, along rail tracks at a train station, metro station, or tram stop, at which passengers may board or alight from.

Prioritization. Process of using risk assessment results to identify where risk reduction or mitigation efforts are most needed and determination of which protective actions should be instituted in order to have the greatest effect.

Progressive collapse. A chain reaction failure of structural members to an extent disproportionate to the original localized damage. Such damage may result in upper floors collapsing onto lower floors.

Rapid transit. Electric railway characterized by high speed and rapid acceleration. Uses passenger railcars operating singly or in multiple unit trains on fixed rails, operates on separate rights-of-way from which all other vehicular and foot traffic are excluded, and uses sophisticated signaling systems and high platform loading.

Replacement value. Current market cost to construct the asset.

Resilience. Ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.

Resilience Score. A numeric value that describes the ability of a mass transit station to resist, absorb, and recover from a potentially disruptive event at a mass transit station.

Risk. Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Risk score. Numerical value obtained from the IRVS that describes the risk to a station for a terrorist attack or natural disaster

Sector. Logical collection of assets, systems, or networks that provide a common function to the economy, government, or society.

Signal. Provides information to the train driver about the line ahead.

Signal box. Building or room that houses signal levers or a control panel.

Social impact. Psychological effect on public morale and confidence as a result of an event.

Stand-off distance. Distance maintained between a building and the potential location for an explosive detonation or other threat.

Subway. Underground railroad, generally in a large city. Considered heavy rail because it operates on a dedicated track.

Target density. Number of potential high-value targets surrounding a mass transit station.

Terrorism. Unlawful use of force and violence against persons or property to intimidate or coerce a government, civilian population, or any segment thereof in furtherance of political or social objectives.

Third rail. Rail running parallel to one of the two running rails of a track; carries a supply of electricity used to power electric cars or locomotives.

Threat. Natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Threat rating. Likelihood or potential of the occurrence of manmade or natural hazard.

Transportation hub. Place where passengers and cargo are exchanged between vehicles or transport modes. Includes train stations, mass transit stations, bus stops, tram stops, airports, and ferry slips.

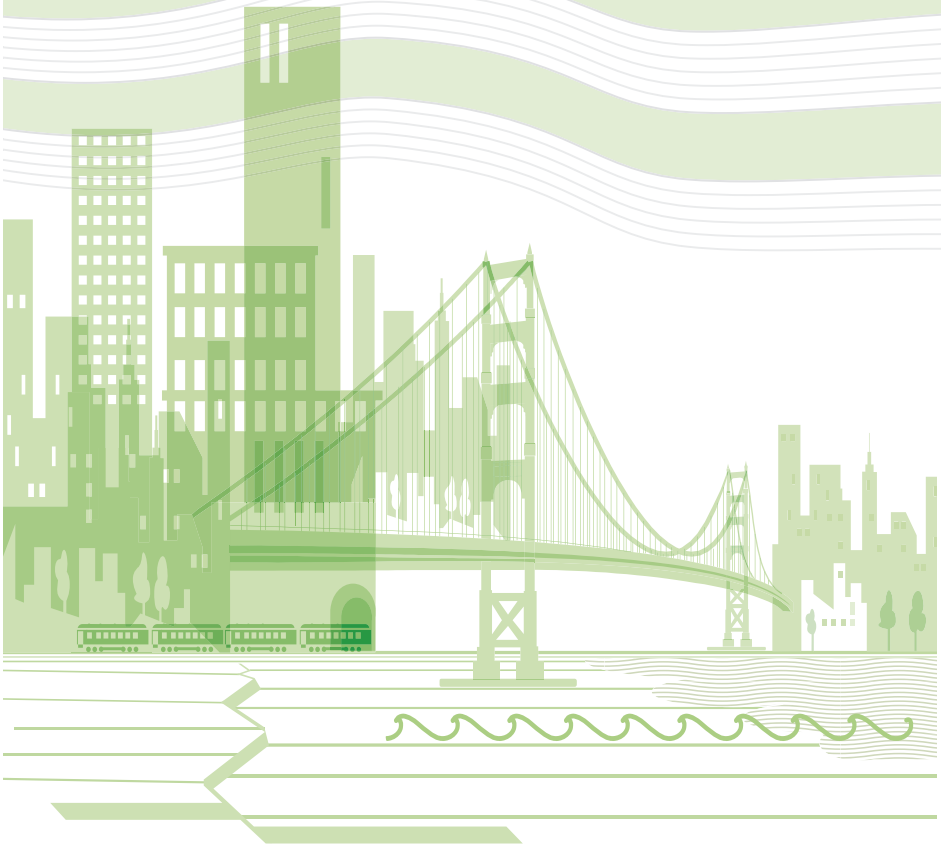
Vulnerability. Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

Vulnerability rating. Weakness of functions, systems, and sites in regard to a particular threat/hazard.

Yard. System or grouping of tracks connected to, but not part of, a main line; used for switching or storing cars, or making up trains.

C

Integrated Rapid Visual Screening (IRVS) Database User Guide



Section 1: Overview and Installation

- **Introduction**
- **Database Overview**
- **System Requirements**
- **Installation Process**

Introduction

This database application is provided to support the Integrated Rapid Visual Screening (IRVS) methodology. The database, titled IRVS Database, is a multi-purpose tool that currently supports IRVS screenings of 1) Mass Transit Stations, 2) Buildings, and 3) Tunnels. This User Guide provides information on how to install the database, use the database to conduct an IRVS screening and to perform system administrative functions.

Database Overview

The IRVS Database is a standalone application that is both a data collection tool and a data management tool. Screeners can use the tool to assist in the systematic collection, storage and reporting of IRVS data. It has functions, folders and displays to collect and display screening data, risk summary scores, digital photos, site plans, floor plans, emergency plans, and certain GIS products as part of the IRVS record of screenings. Managers can use the application to store, search and analyze data collected from multiple screenings, and then print a variety of reports.

The IRVS Database is a standalone application that is both a data collection tool and a data management tool.

The database is designed for an organization to transfer screening information between two or more copies of the database: one (or more) copies of the database loaded on the screening team laptop(s) and for collecting data in the field; and one copy of the database loaded on a computer at an organization's headquarters for collecting the results, printing reports, and analyzing the information from a number of screenings. The temporary database used in the field by a screening team is referred to in this guide as the Field Database. The primary database copy at an organization's headquarters is referred to in this guide as the Master Database.

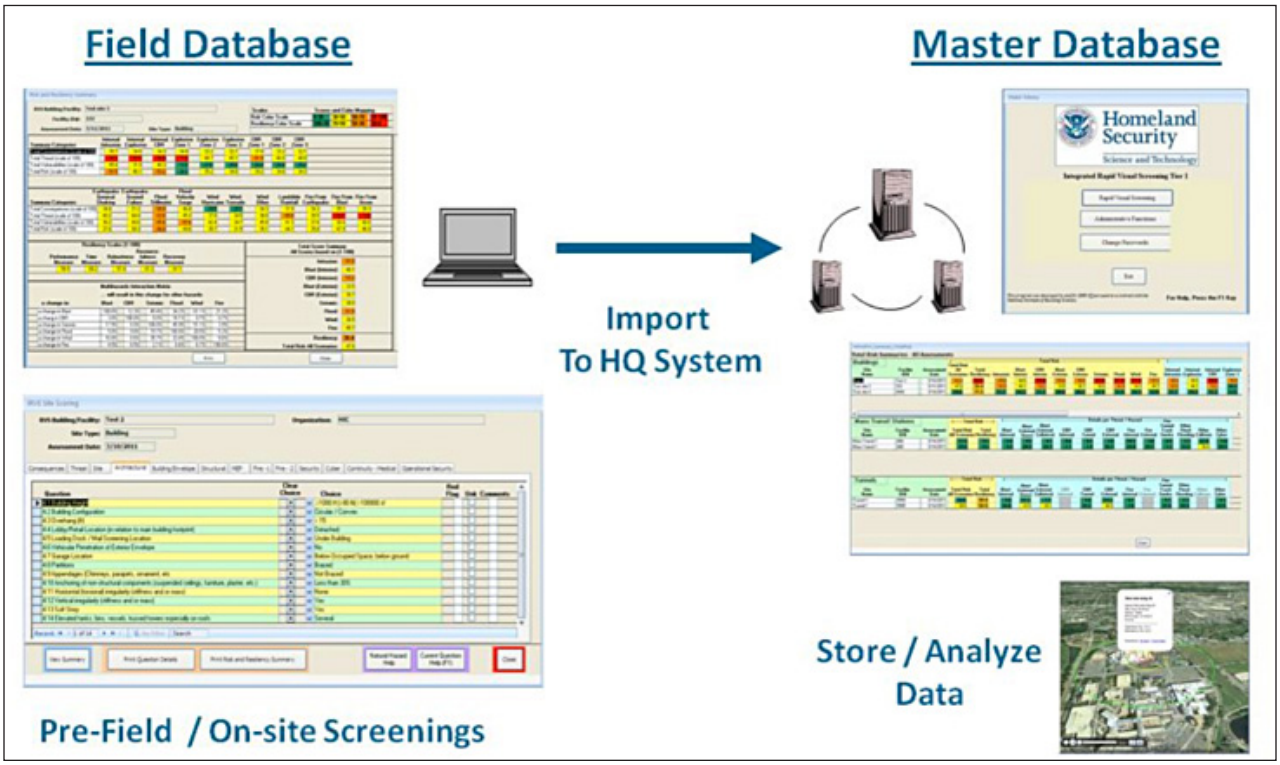
The database on a screener's laptop, referred to in this guide as the Field Database, is used to perform the following functions:

- Create the screening record, to include site identification, address, sector and subsector identification, site importance, and geographical coordinates
- Create an Executive Summary of the screening as well as a list of the screening team and site points of contact
- Record Pre-Field data entry: Hazards, Pre-Field Questions, and Structure Type.
- Record Site Evaluation data entry
- Display the site's Risk Summary
- Create folders and displays of collected digital photos, site plans, floor plans, emergency plans, and certain GIS products
- Transfer the collected IRVS data to the organization's Master Database
- Purge the collected data from the Field Database laptop and prepare it for subsequent screenings

The primary database at an organization's headquarters, referred to in this guide as the Master Database, is used by managers to store, search print, display and analyze data collected from multiple screenings. Capabilities include:

- Import collected IRVS data from Field Team databases
- Store, search and analyze data on multiple IRVS screenings
- Display and print a variety of reports
- Identify mitigation strategies
- Create a duplicate of an IRVS record for mitigation analysis or "What if" impacts resulting from changes to the Consequence, Threat, Vulnerability and Resiliency status
- Produce standard reports or export report data as a MS Word® or PDF® document for additional editing and formatting
- Export screening risk data to MS Excel® spreadsheets for additional editing and tracking
- Filter and sort screening records by site identification, address, sector and subsector identification, and facility importance
- Plot and display IRVS screening sites and risk values on the users digital mapping program
- Display the Total Risk Summary for one site or for a filtered list of sites.

- Store, display, and print collected digital photos, site plans, floor plans, emergency plans, certain GIS products, and other miscellaneous files collected during screenings
- Perform Database Administrative functions



System Requirements

The following are the hardware and software requirements for the basic IRVS Database:

- Pentium® 4 or equivalent processor
- Windows XP®
- MS Access® 2003 or later
- MS Excel® 2003 or later
- 256 MB of RAM recommended for all components
- Adobe Reader®

The database has an optional plotting function to display IRVS site coordinates and screening information on a digital map. The plotting function requires the use of a systems existing mapping program capable of displaying a KML type file, such as Google Earth® . (Keyhole Markup Language (KML) is an XML-based language for defining the display of three-dimensional spatial data in the programs like Google Earth®.)

Reminder: the database must be opened using the shortcut installed during the initial setup.

Installation Process

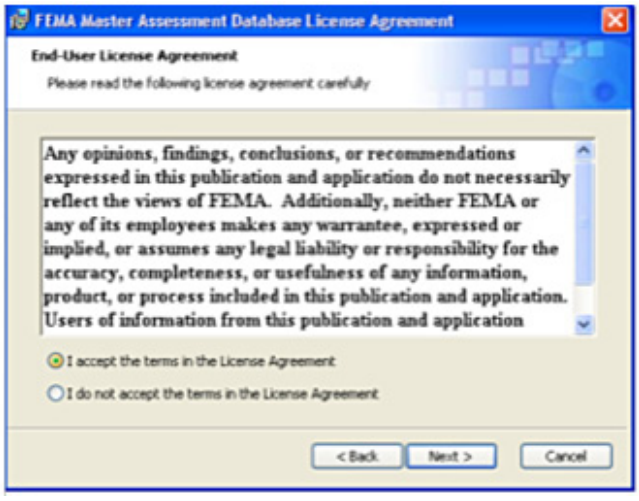
Download and install the database program from the DHS website: XXXXXXX. Follow the download and self installation instructions on the DHS website. It is recommended to install the database on two separate systems: one to use as the IRVS Master Database and one to use as a temporary database on an IRVS screener's system.

After downloading the program, begin the installation process by first closing all other programs and then double left click on the SETUP.EXE file. Note: If the program was previously downloaded to you computer, left click **Start, Run**, identify the location where the SETUP.EXE program can be found (CD, C:/Temp, or some other storage location on hard drive or media) and then left click on the SETUP.EXE file.

Install Wizard

The Install Wizard first identifies the name of the software being installed. Left click **Next** to continue after confirming that this is the software you want to install.

NOTE THESE ARE PLACE HOLDER PICTURES



End User License Agreement (EULA)

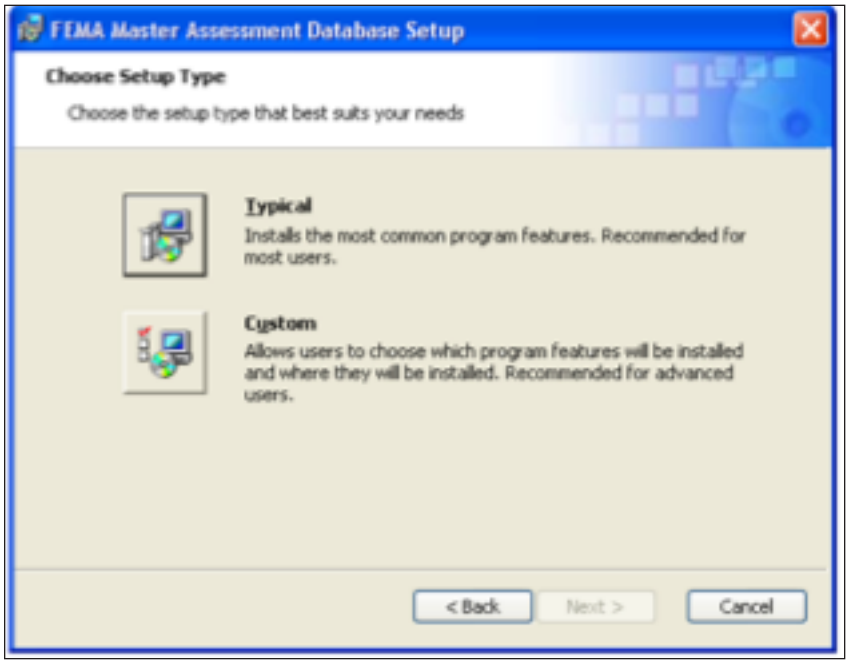
A standard screen showing the End User License Agreement will appear. Read as you feel appropriate, then left click on the **Accept** circle, and left click on **Next** to continue with the installation.

Customer Information

Add the User Name and Organization in the appropriate windows. Continue with the installation by left clicking Next.

Typical Installation

There is no advantage in using the Custom Installation. There are no component programs to select. The only feature that the Custom Installation allows is to change the file name and/or file location. In most cases you should follow the Typical Installation. To proceed, left click on **Typical**.



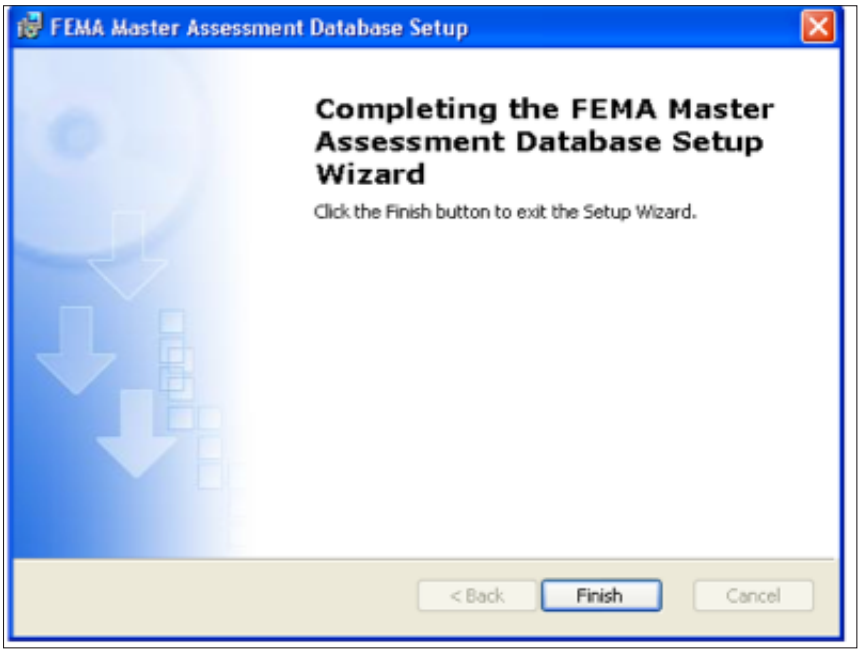
NOTE THESE ARE PLACE HOLDER PICTURES

Installation Completion

A standard screen to ensure you are ready to install will appear. Proceed by left clicking **Install**.

Depending on the configuration of your system, the Install Wizard may take a long time looking for it and display a searching flashlight. It should eventually find it and get to this screen. The final standard screen indicates the Install Wizard has completed the installation. Left click **Finish** to end the installation.

NOTE THESE ARE PLACE HOLDER PICTURES



Following the same procedure, install a additional copy of the program for use on the computer(s) that your IRVS screeners will use to collect data, such as a laptop.

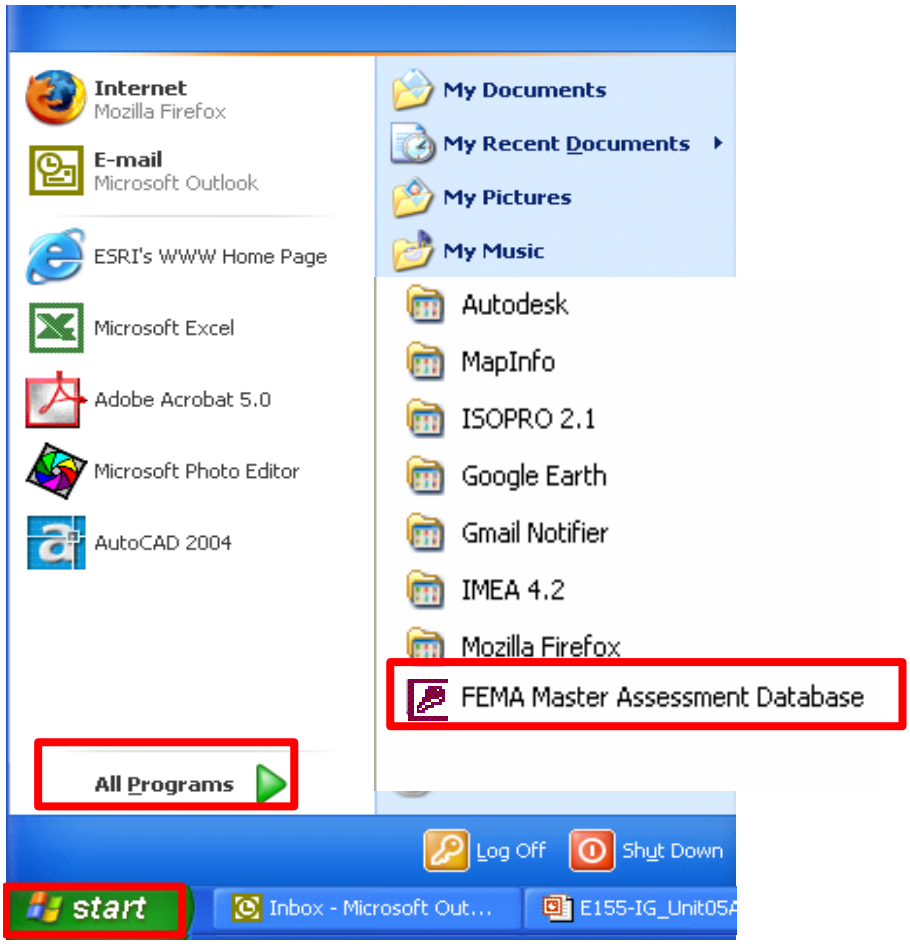
Section 2: Open and Start the IRVS Process

- **Open and Login to the IRVS Database**
- **IRVS Database Main Menu**
- **Help Function**

Open and Logon to the IRVS Database

To open the IRVS Database, you first left click on **Start**, then **Programs**, and look for the **IRVS Database** to left click. The IRVS Database should be at the end of the Startup Program Menu immediately after the installation. You can copy the shortcut icon for the IRVS Database to another location at any time.

Note: the database can only be opened by left clicking on the IRVS Database Icon.



NOTE THESE ARE PLACE HOLDER PICTURES

Logon to the Database

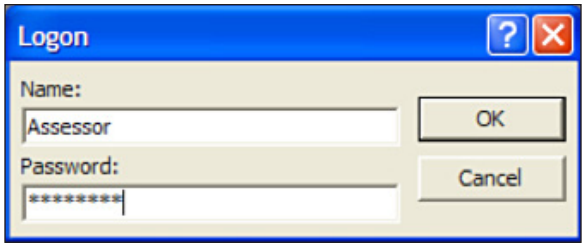
The first action to enter the database is to logon with a user name and password. You can enter a newly installed IRVS database with the user names of: **Assessor**, **Editor**, **Reader** or **Administrator**. It is recommended to open the database the first time using the **Administrator** logon name which provides access to all functions of the program. The initial password for the **Administrator** user name is "Administrator". (Do not include the quotation marks, i.e. " ", in the user name or password.) By logging in with the **Administrator** user name, you will be able to establish new user accounts and passwords. (Explained further in, Section 8: Administrative Functions, of this manual.) If new user names and passwords have already been assigned, use your assigned user name and password to enter the database.

The database is preloaded with the following four user names and passwords:

- **Name:** Administrator **Password:** Administrator
- **Name:** Assessor **Password:** Assessor
- **Name:** Editor **Password:** Editor
- **Name:** Reader **Password:** Reader

NOTE THESE ARE PLACE HOLDER PICTURES

These passwords are examples only and should be changed after installing the program (you will learn how to do this later in this guide).



Enter your user name in the **Name** window and your password in the **Password** window, and then left click on **OK**.

This leads to a **Main Menu** of the database.

IRVS Database Main Menu

The **Main Menu** of the database provides five options to the User:

- Conduct **IRVS Screenings** by left clicking on the <**Rapid Visual Screening**> button. This opens the IRVS module of the database. All screeners have access to this module.
- Perform **Administrative Functions** by clicking on the <**Administrative Functions**> button.

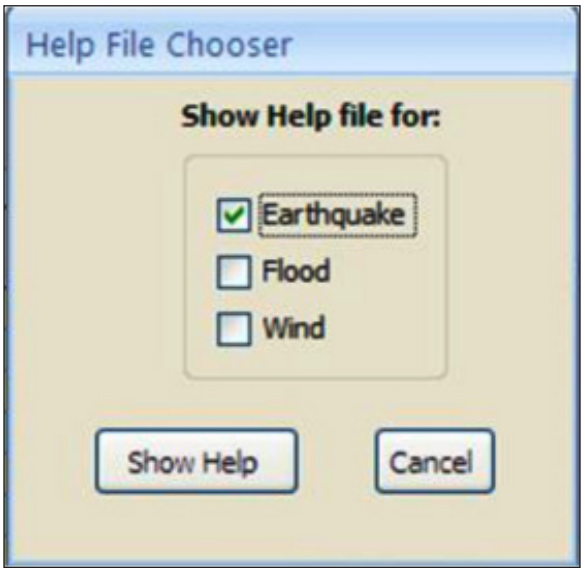
Note: administrative functions are not available to all users. Only those logged on with administrator permission can use the administrative functions. For example, only administrators may import screening records from the field database copy to the Master Database copy

- Change the **Password** of the user that is logged on by clicking on the <**Change Password**> button. All users have access to change their own password.
- Start the basic IRVS module by left clicking on <**Rapid Visual Screening**> button.

Help Function

On all forms in the database, the user guide or a specific catalog reference can be opened by first left clicking on an area or question in a form, and then selecting the F-1 key on the user's key board.

Current Question Help: The user guide or a specific catalog reference can be also be opened by left clicking the <**Current Question Help** [F1]> button on the bottom of many forms.



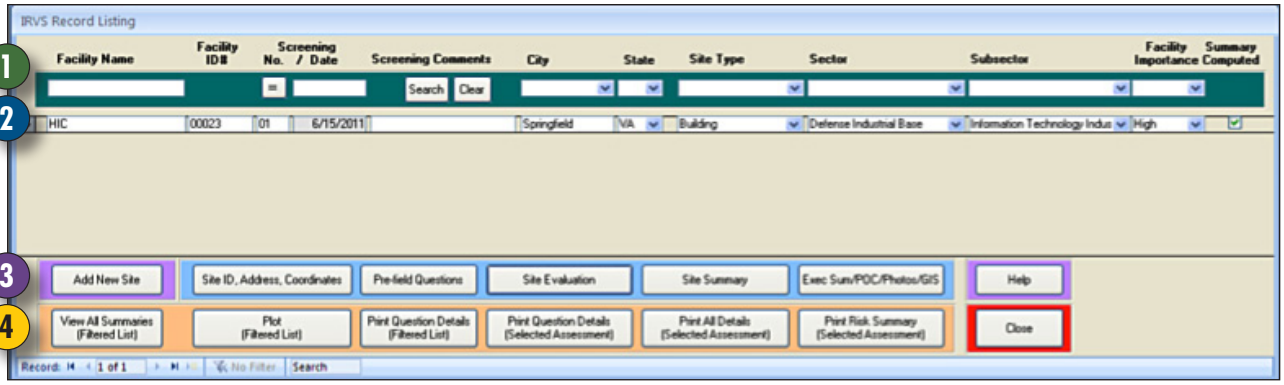
Natural Hazard Help: A specific catalog reference can be also be opened by left clicking the <**Natural Hazard Help**> button on the bottom of the two Site Scoring forms. This opens up a separate window and enables the user to display special help files for the topics of: Earthquake, Flood, and Wind.

Section 3: Create and Display an IRVS Record

- **IRVS Record Listing**
- **Create a new IRVS Record**
- **Plot/Display IRVS Site Coordinates**
- **Facility Screening Folders**

IRVS Record Listing

Selecting the <**Rapid Visual Screening**> button from the Main Menu will bring you to the **IRVS Record Listing** form. This displays a list of the current screening records in the database. The first time you enter the database (with no prior screenings entered), this list will be blank. From this form you can either add a new IRVS record or review/edit a record previously entered screening.



There are four areas on this form:

- The top section of the form (marked with a 1 in the diagram) enables the user to sort the list of records. Enter a search term or use the drop down boxes under one or more columns to create a query. Then left click the <**Search**> button to filter the records and display a list of only those records that match the query. Left click the <**Clear**> button to clear the query and display all records in the database.
- The second section of the form (marked with a 2 in the diagram) enables the user to select a single record to display or edit. First select one of the records in the list by left clicking on the far left column. This will mark the screening record desired with a right pointing arrow head if one is not already there. This selects the screening record and links the buttons on the form to that screening.

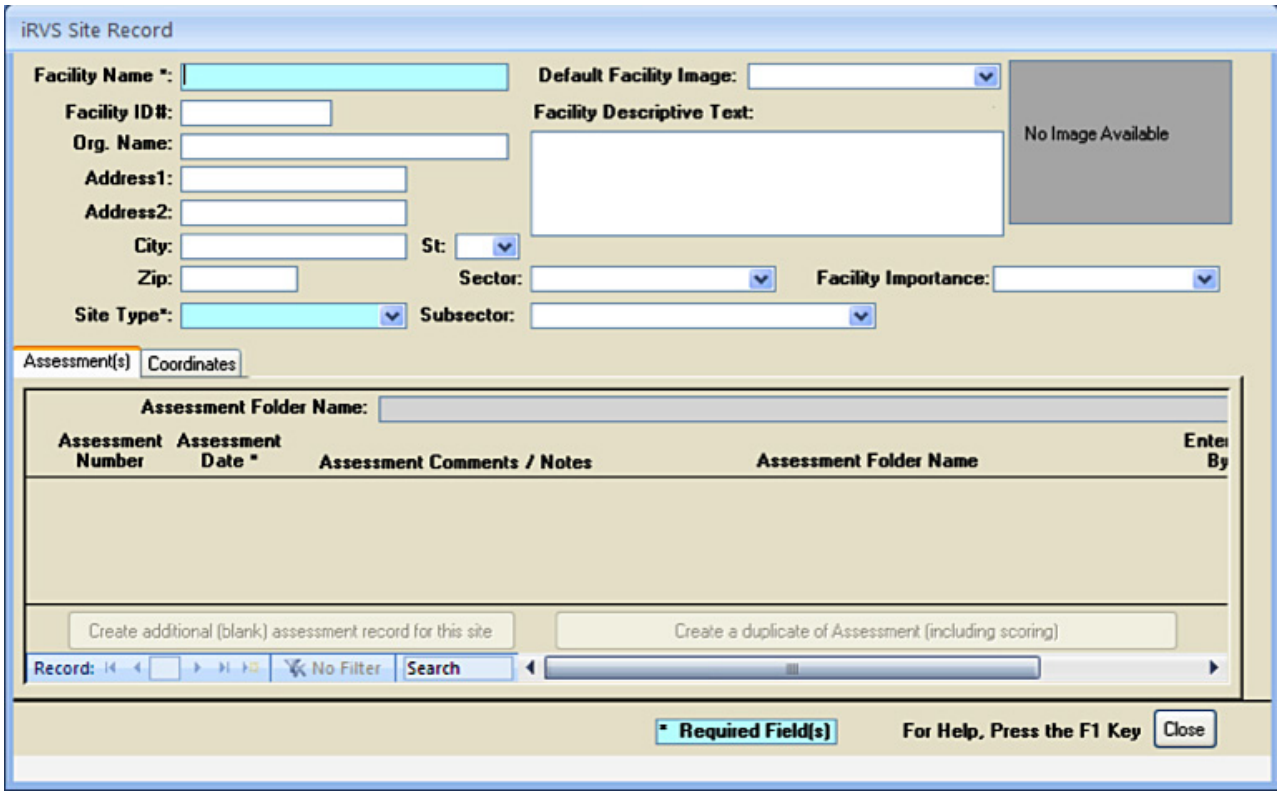
- The third section of the form (marked with a 3 in the diagram) enables the user to create a new IRVS record for screening, to conduct a evaluation of the selected record, to display the Risk Summary of the selected record, and to enter/edit additional information, photos, and files of the selected record.
- The bottom section of the form (marked with a 4 in the diagram) enables the user to display, plot, and print screening details for multiple screening records.

Create an IRVS Record

The first task for using the database is to create a new IRVS record. This establishes a record in the database and stores the basic information about the site to be screened including: screening date, site name, site unique ID number, address, sector and subsector identification, site importance, and geographical coordinates.

To create a new IRVS record:

- Left click on the <**Add New Site**> button in the lower left corner. The software will immediately go to the <**IRVS Site Record**> screen.



On this screen, information about the screening site is recorded. This information is used to produce IRVS reports and for filtering during queries. Note the three asterisked (*) entries: **Facility Name**, **Site Type**, and **Screening Date**. These three fields are the minimum required entries to create an IRVS record. The other fields are optional.

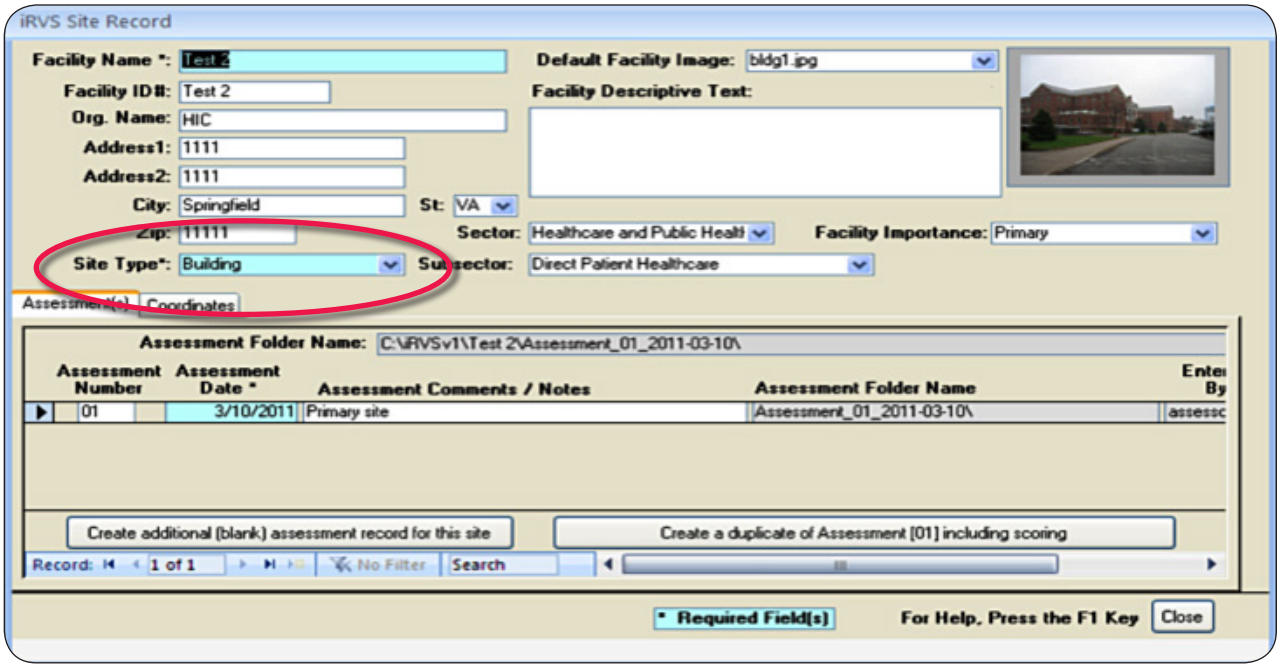
- **Name and Address:** The name and address fields are simple text entry boxes. Note you may select the state from a drop down menu, or type in the two letter abbreviation.
- **Facility Descriptive Text:** simple text entry box.
- **Sector and Subsector:** The Sector and Subsector fields are drop down entries. Select the Sector entry first. The Subsector choices are populated from the Sector selection.
- **Facility Importance:** The Facility Importance field is a simple drop down list with three choices: High, medium, Low. There are no predefined criteria for these rankings. This field is simply provided as an additional means for a organization to filter and query screening records.
- **Default Facility Image:** The Default Facility Image is a drop down box listing of pictures loaded into the database for this screening site. Select one picture and it will display on the form when the record is opened.
- **Site Type:** The Site Type field is a drop down list with three choices: Buildings, Mass Transit Systems, and Tunnels.

The "**Site Type**" field may need some further clarification. The RVS tool provides tailored question sets and risk calculations for different types of infrastructure. Currently, the IRVS tool supports three different types of infrastructures: Buildings, Mass Transit Systems, and Tunnels. For each record the user must identify the type of infrastructure to be screened by selecting from the drop down box "Building", "Mass Transit Station", or "Tunnel".

Currently, the IRVS tool supports three different types of infrastructures: Buildings, Mass Transit Systems, and Tunnels.

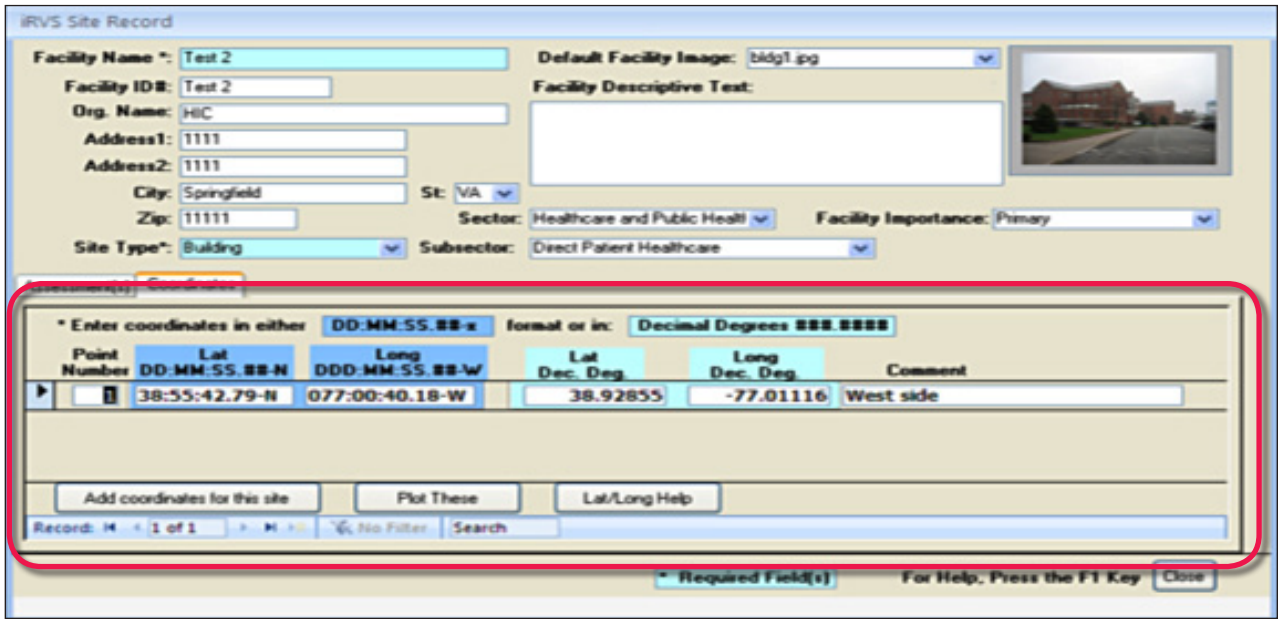
After selecting a **Site Type**, the software enables the two Tabs on the form: **Screening Records** and **Coordinates**.

- The **Screening Records Tab** enables the user to either create a new blank record (with no previously entered evaluation data) for this site or to create a duplicate of an existing IRVS record (with evaluation data)for use in analysis or "What if" investigation.
- The **Coordinates Tab** enables the user to record coordinates around the screening site and plot them on the users mapping program.



Plot/Display IRVS Site Coordinates

The **Coordinates Tab** enables the user to record coordinates of the screening site and plot them on the users mapping program. This visualization tool not only enhances the screening evaluation collection process, but also supports the risk analysis process and post IRVS mitigation planning. (Note: the user must have an installed imagery program compatible with reading KML files, such as Google Earth®, on their system to use the Coordinates function.



To create a plot point, enter the point's Latitude and Longitude values on the **Coordinates Tab**. Multiple plot points can be added by simply left clicking the <**Add Coordinates for this site**> button. The database automatically assigns a point number to each plot.

Note: You can enter coordinates in either in Degrees Minutes Seconds format or in Decimal Degree format; however values in Decimal Degree format are used to create the KML file for display in Google Earth® or other visualization program.

If you have coordinates in Degrees Minutes Seconds format, enter them in the first two boxes, and the Decimal Degree equivalents will be calculated for you in the second two boxes.

Alternatively, you can enter the Decimal Degree values directly in the second two boxes. If you choose to do this, then any values that might have already be in the corresponding Degrees Minutes Seconds fields will be removed, leaving only the Decimal Degree values you supplied.

Left clicking the <**Plot These**> button generates a KML file and automatically opens the file for visualization of the screening site.

- The process plots the entered coordinates and displays a 100 ft., 300 ft., and 1,000 ft. ring around the plotted points
- The process also displays the following IRVS screening information about the site:

Name: _____

Site Type: _____

Sector: _____

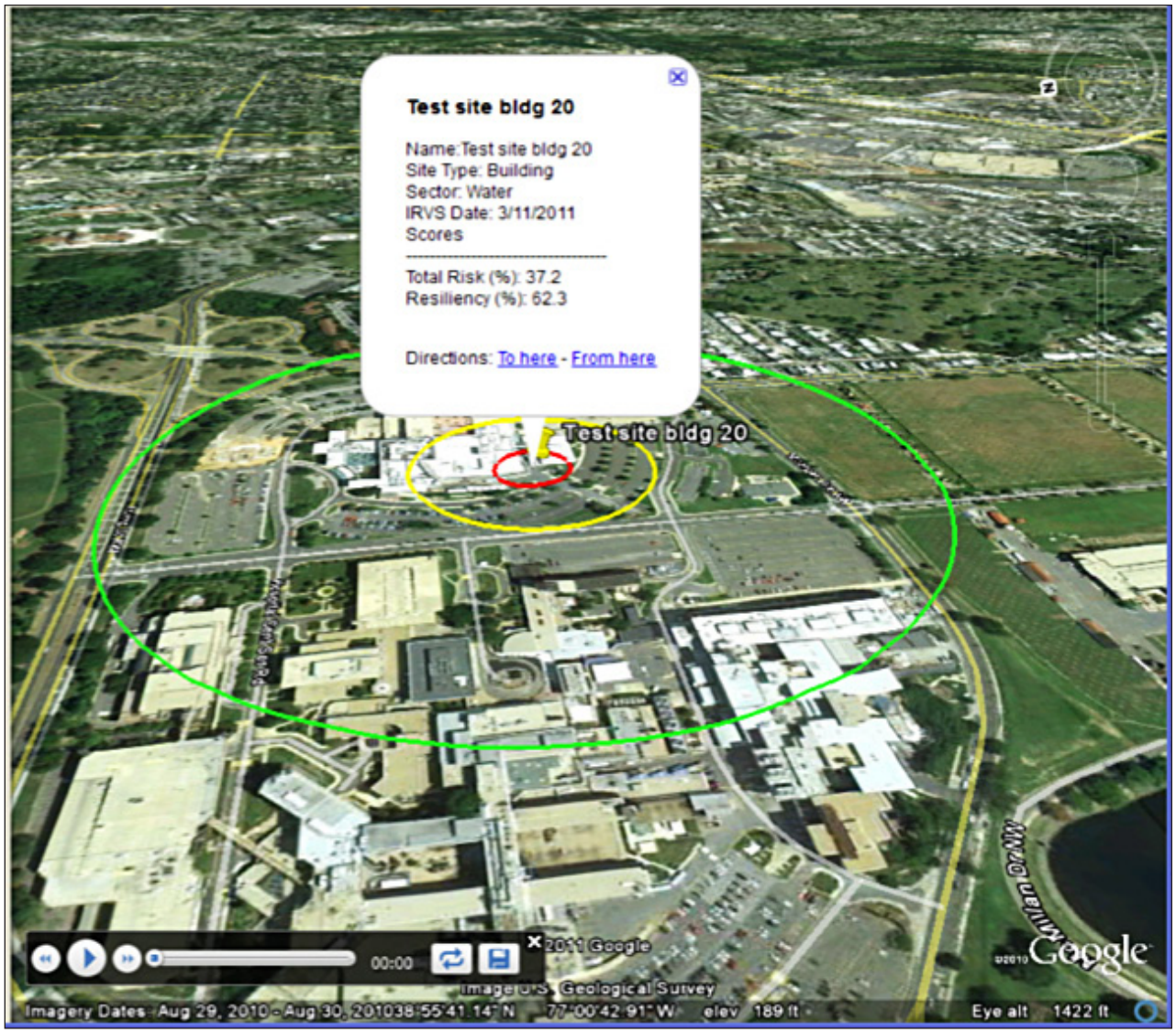
IRVS Date: _____

Scores _____

_____

Total Risk (%):_____

Resiliency (%): _____



Facility Screening Folders

When you create the new IRVS record, the software automatically creates three subfolders named GIS Portfolio, Miscellaneous Files, and Photos, all under a main folder that uses the IRVS Site location and screening date as the main folder name.

The record's folder name is automatically displayed in the field "**Screening Folder Name**". The program will also display a reminder notice of the folder location when you create the screening record. After taking notice of folder names, left click **OK** to finish creating the record.

Note: If you changed the program's location using Custom Installation, then you should make note of the file path that these subfolders are placed in, as you will need that information to properly load and link the contents of these subfolders to other databases.

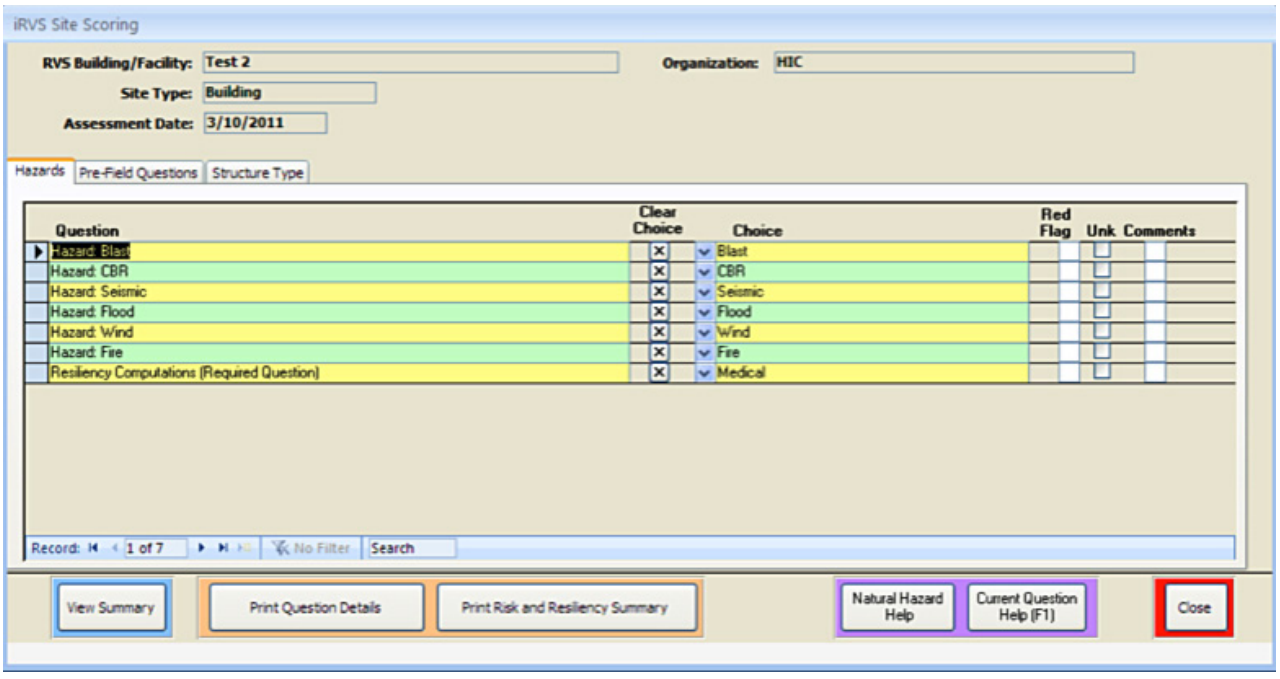
Section 4: Conduct an IRVS Screening

- **Using the IRVS Data Forms**
- **Conduct Pre-Field Data Entry**
- **Conduct an On Site Evaluation**
- **Calculate and Review the Risk and Resiliency Summary Screen**

After you have created an IRVS site record, you are ready to start the IRVS screening process. First select one of the screening records by left clicking on the far left column of the **IRVS Record Listing** form. This will mark the screening record desired with a right pointing arrow head if one is not already there. This selects the screening record and links the buttons on the form to that screening record.

Using the IRVS Data Forms

The tabs on the Pre-Field and Site Evaluation forms function in a similar manner. There is a list of question fields on the left side of the form followed by a response field drop down list. Each question also has a Clear Choice "**X**" button, and a "**Red Flag**", "**Unknown**" and "**Comment**" entry box.



- The first column is a series of questions.
- To the right of each question, under a column titled "**Choice**", is a drop down list of possible answers. Make your selection by left clicking on your answer.
- To the right of the Question field is a button with an "**X**". By left clicking on this button, the previously entered choice for that single row will be cleared allowing the assessor to select a new response. Note that this action does not remove the marking in the red flag or unknown box, nor a comment. This must be accomplished separately.
- The box under the column "**Red Flag**" should be marked when the screener determines the circumstances surrounding the response to a question may be a concern requiring immediate attention.
  1. Left click in the box to mark the question with a red flag.
  2. A red flag generates a mandatory comment field to support the screener's decision. Left click on **OK** to enter the comment.
  3. Enter your comments in the box, and then left click on Save.
  4. To remove a red flag, left click on the red flag.
- The box under the column "**Unknown**" is marked if the screener does not know the answer at the time of the screening. This can be changed at a later time when the proper response is learned. To remove a check mark in the "**Unknown**" box, left click on the check mark.
- The box under the column "**Comment**" is marked at any time to support or explain a unique or extraordinary circumstance. A comment is mandatory when the "**Red Flag**" box is marked.
  1. To add a comment, left click in the "**Comment**" box.
  2. Enter your comments in the box, and then left click on **Save**.
  3. To remove a comment, left click on the "**Comment**" box.
  4. Delete the comment and left click the **Save** button.
  5. The box will no longer be marked. Edit the comment in the same manner but the box will remain marked.

Across the bottom of the Pre-Field and Site Evaluation forms are Six buttons used to view and print IRVS data and also to view Help screens.

- View Summary: The <View Summary> button displays the Risk and Resiliency Summary form.
- Print Question Details: The <Print Question Details> button opens to a print view screen and displays a report consisting of the IRVS questions and answers. Note this view does not include the Risk and

Resiliency Summary screen or the other details of the screening (such as POC listing, Screening Team members, executive summary).

- **Print Risk and Resiliency Summary:** The <**Print Risk and Resiliency Summary**> button opens a Print Per-view screen of the Risk and Resiliency Summary.
- **Natural Hazard Help:** A specific catalog reference can be also be opened by left clicking the <**Natural Hazard Help**> button on the bottom of the two Site Scoring forms. This opens up a separate window and enables the user to display special help files for the topics of: Earthquake, Flood, and Wind.
- **Current Question Help:** The user guide or a specific catalog reference can be opened by first left clicking on an area or question in a form, and then left clicking the <**Current Question Help** [F1]> button.
- **Close:** The <**Close**> button returns the user to the previous menu.

Conduct Pre-Field Data Entry

Pre-field data is the information that should be gathered before the onsite field screening is conducted. It is important to emphasize that screeners should make the effort to complete, as much as possible, the information required in the pre-field data in order to obtain accurate scorings.

The information gathered in the pre-field screening is intended to document basic identification and target density (described in the following section) information.

The pre-field data may be directly obtained from the screeners existing knowledge of the asset or through various private or public sources on the Internet.

Left click on the <**Pre-field Questions**> button to review or edit information. The software will immediately go to the Pre-field Scoring Form. Note the Pre-field form is tailored to the Site Type previously designated: Buildings, Mass Transit, or Tunnels.

- For Mass Transit and Tunnels, the Pre-Field form displays only one Tab: Per-Field Questions
- For Buildings, the Pre-Field form displays three Tabs: Hazards, Pre-Field Questions, and Structure Type.

Hazard Tab (Building Screening Only)

The **Hazards Tab** enables the screener to tailor the Building screening process. The Screener designates of Hazards to include in the process and if Resiliency Computations are also to be included in the process.

The first five questions are a list of hazards:

- Blast
- CBR
- Seismic
- Flood
- Wind

Choose to include or not to include each of these Hazards.

The sixth hazard listed, "Hazard: Fire" is also used to tailor the IRVS screening. There are three choices for this hazard:

- **Short fire vulnerabilities checklist:** Fire Tab 1 will be displayed if this is selected. It has a small set of questions related to the hazard of fire will be included in the screening.
- **Fire marshals list - Longer list - includes all short list attributes:** Fire Tab 2 will be displayed if this is selected. This is a larger detailed set of fire related questions. If the screener wants to expand the basic question set and answer a larger detailed set of fire related questions, they may indicate that choice by selecting this option.
- **Blank space:** Chose this selection if you do not want to include the hazard "Fire" in the screening.

The IRVS screening is adjusted based on which Hazards are selected. At the completion of this form, the database automatically tailors the IRVS question set and grays out un-needed questions. Only those hazards selected are included in the risk analysis.

The final question listed on this form, "Resiliency Computations (Required Question)" is also used to tailor the IRVS screening. The answers provided in the drop screen are as follows

- **No resiliency computations are needed:** if this answer is selected, the resiliency sections of the IRVS methodology will be omitted from the screening. No resiliency related Tab will appear during the site evaluation scoring.

- **General:** if this answer is selected, the resiliency sections will be tailored to screen general facilities such as: commercial, agricultural, educational, and industrial. A "Continuity – General" Tab will appear during the site evaluation scoring.
- **Government:** if this answer is selected, the resiliency sections will be tailored to screen government facilities such as: offices, police stations, fire stations, and emergency operations centers. A "Continuity – Government" Tab will appear during the site evaluation scoring.
- **Medical:** if this answer is selected, the resiliency sections will be tailored to screen medical facilities. A "Continuity – Medical" Tab will appear during the site evaluation scoring.
- **Schools (K-12):** if this answer is selected, the resiliency sections will be tailored to screen school facilities. A "Continuity – School (K-12)" Tab will appear during the site evaluation scoring.
- **Business/Financial:** if this answer is selected, the resiliency sections will be tailored to screen/Business/Financial facilities. A "Continuity – Finance/Business" Tab will appear during the site evaluation scoring.
- **Retail:** if this answer is selected, the resiliency sections will be tailored to screen retail facilities. A "Continuity – Retail" Tab will appear during the site evaluation scoring.

Pre-Field Questions Tab

The Pre-Field Questions Tab displays a tailored list of questions that starts the IRVS screening process. The questions displayed are adjusted based on the type of infrastructure (Tunnel, Building, or Mass Transit) and the hazards selected (Blast, CBR, Seismic, Flood, Wind, and /or Fire). Those questions that are not needed are grayed-out and not included in the risk analysis.

Structure Type Tab (Building Screening Only)

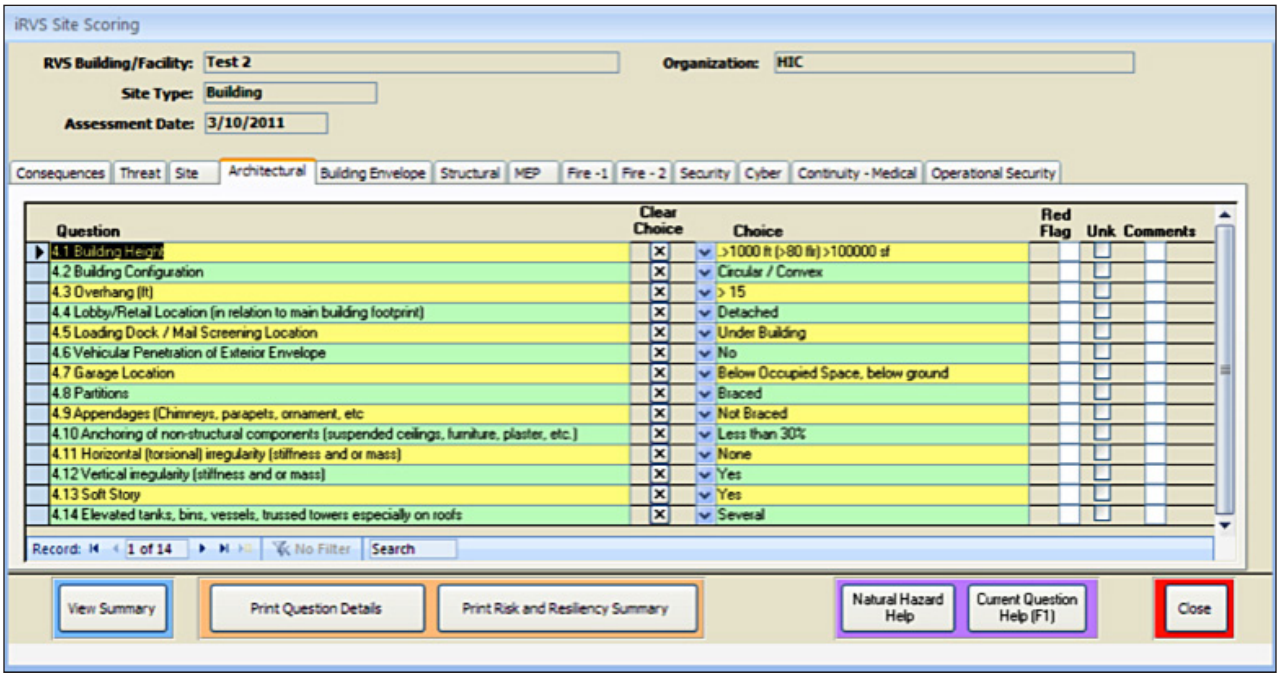
The Structure Type Tab is only displayed when screening a building. The one question displayed on this Tab, "Building Type" is a critical question for the IRVS methodology. The screener should refer to the Building catalog when trying to determine the building type. The catalog can be opened by first opening the Structure Type Tab and then selecting the F-1 key on the user's key board. The catalog can be also be opened by left clicking the <**Current Question Help** [F1]> button on the bottom of the form.

Conduct on Site Evaluation

After you have completed Pre-field data entries, you are ready to record the IRVS on site screening data. First select one of the screening records by left clicking on the far left column of the IRVS Record Listing form. This will mark the screening record desired with a right pointing arrow head if one is not already there. This selects the screening record and links the buttons on the form to that screening record. Next left click the <**Site Evaluation**> button to open the IRVS Site Scoring Form.

The IRVS Site Scoring form is used to record answers to a series of screening questions on 11 to 14 Tabs. The question set and number of Tabs displayed are adjusted based on the users previous selections: the type of infrastructure (Tunnel, Building, or Mass Transit); the hazards selected (Blast, CBR, Seismic, Flood, Wind, and/or Fire); and Resiliency selection (No Resiliency computations, Governmental, General, Medical). Questions that are not needed are grayed-out and not included in the risk analysis.

The Questions and tabs on the IRVS Site Scoring forms are set up in a similar manner to the Pre-Field form. There is a list of question fields on the left side of the form followed by a response field drop down list. Each question also has a Clear Choice "**X**" button, and a "**Red Flag**", "**Unknown**" and "**Comment**" entry box.



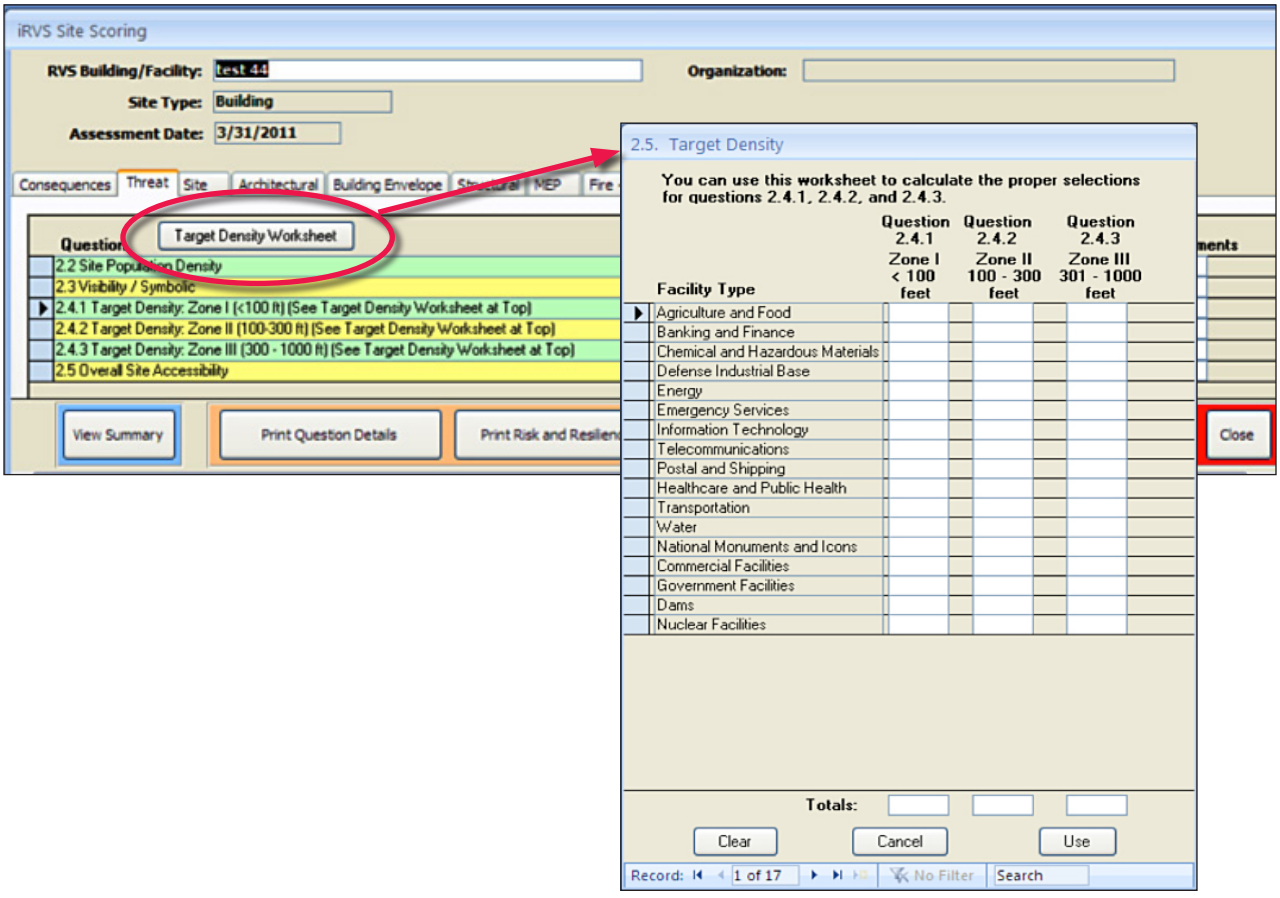
Threat Tab: Target Density Zones

The Threat Tab contains a special Help button labeled <**Target Density Worksheet**> at the top of the question list. The Help file is specific to three questions on the Tab

- Question 2.4.1 Target Density Zone I (<100ft)
- Question 2.4.2 Target Density Zone II (100-300ft)
- Question 2.4.3 Target Density Zone III (300-1,000ft)

Responses to these three questions can either be entered from the drop-down menu of each question or the assessor can use the Target Density Zone Worksheet to answer the questions.

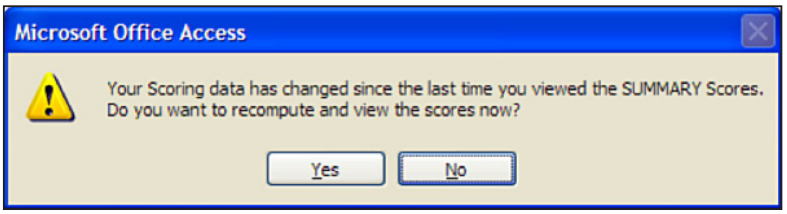
Left click on the <**Target Density Worksheet**> button at the top of the question list and a table labeled "**Target Density**" will pop-up. The assessor can use the worksheet to calculate the proper selections for questions 2.4.1, 2.4.2, and 2.4.3enter the exact number of facilities for each category and zone into the table. After completing the table, left click the <**Use**> button to automatically populate the answers to the three questions.



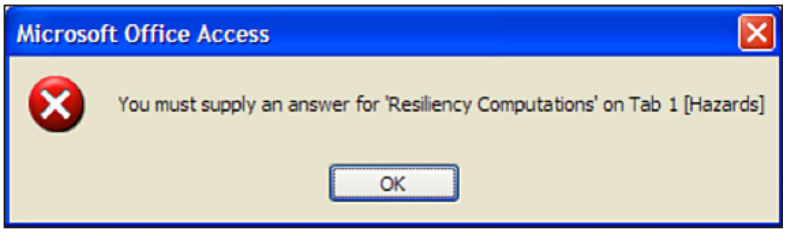
Calculate and Review the Risk and Resiliency Summary Screen

After completing the Pre-Field and Site Evaluation data entry, use the <**View Summary**> button on the IRVS Site Scoring form or the <**Site Summary**> button on the IRVS Record Listing form to display the Risk and Resiliency Summary Screen. This starts several automated process reviews and risk assessment calculations.

- **Check if Recompilation is Required:** The system first checks if any scoring data has changed since the last time you viewed the Summary Scores. If there has been no change, the system does not need to recompute the data and will simply display the existing **Risk and Resiliency Site Summary**. If scoring data has changed (an answer to a question was added or changed), the system will display the below message stating the **Risk and Resiliency Site Summary** needs to be recomputed. If this happens, left click <**Yes**> to recompute and view the Risk and Resiliency Site Summary.

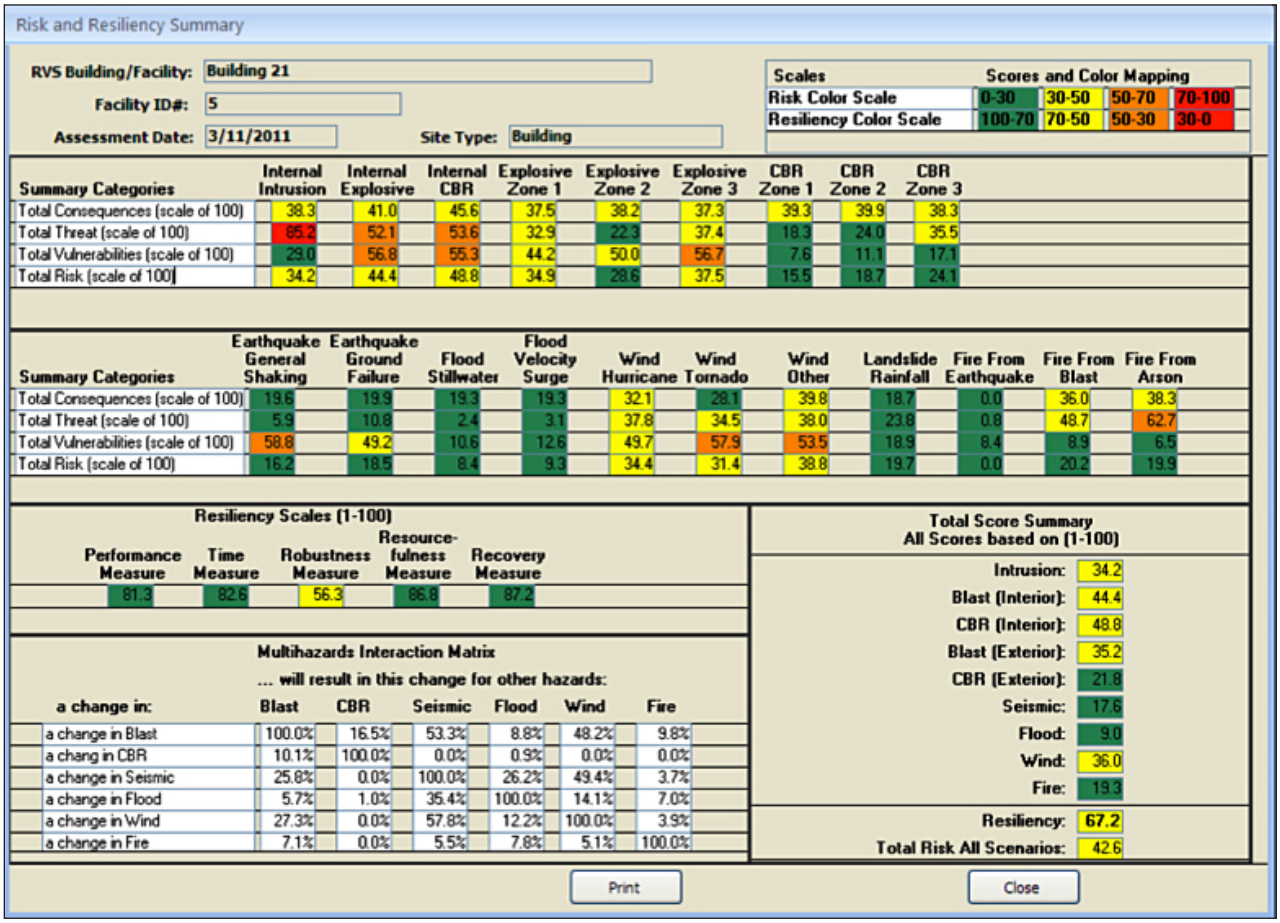


- **Check for Required Entries:** The system next checks to ensure all required entries were entered into the forms. If a required entry is missing, the system will not calculate the **Risk and Resiliency Site Summary** and prompt you to provide the missing answers. For example, if the user does not answer the **Resiliency Computation** question on the Hazards Tab, the system will display the following error message. If this happens, Left click <**OK**> to return to the database and enter the missing data.



- **Check if MS Excel® is Running:** The program next checks if the MS Excel® is currently an open program on your computer. This is done because the database uses MS Excel® to calculate the **Risk and Resiliency Site Summary**. If MS Excel® is an open program, then the system will not calculate the Risk and Resiliency Site Summary and prompt you to close MS Excel®.

- **Calculate Risk and Resiliency Site Summary:** If all required answers are present and MS Excel® is not running, the system will compute the **Risk and Resiliency Site Summary** and display the below message. Note depending on the capability of your computer system, this could take a few moments. After calculations are completed, the system will display the **Risk and Resiliency Site Summary**.



Risk and Resiliency Summary

RVS Building/Facility: Building 21
Facility ID#: 5
Assessment Date: 3/11/2011
Site Type: Building

Scales	Scores and Color Mapping			
Risk Color Scale	0-30	30-50	50-70	70-100
Resiliency Color Scale	100-70	70-50	50-30	30-0

Summary Categories	Internal Intrusion	Internal Explosive	Internal CBR	Explosive Zone 1	Explosive Zone 2	Explosive Zone 3	CBR Zone 1	CBR Zone 2	CBR Zone 3
Total Consequences (scale of 100)	38.3	41.0	45.6	37.5	38.2	37.3	39.3	39.9	38.3
Total Threat (scale of 100)	85.2	52.1	53.6	32.9	22.3	37.4	18.3	24.0	35.5
Total Vulnerabilities (scale of 100)	29.0	56.8	55.3	44.2	50.0	56.7	7.6	11.1	17.1
Total Risk (scale of 100)	34.2	44.4	48.8	34.9	28.6	37.5	15.5	18.7	24.1

Summary Categories	Earthquake General Shaking	Earthquake Ground Failure	Flood Stillwater	Flood Velocity Surge	Wind Hurricane	Wind Tornado	Wind Other	Landslide Rainfall	Fire From Earthquake	Fire From Blast	Fire From Arson
Total Consequences (scale of 100)	19.6	19.9	19.3	19.3	32.1	28.1	39.8	18.7	0.0	36.0	38.3
Total Threat (scale of 100)	5.9	10.8	2.4	3.1	37.8	34.5	38.0	23.8	0.8	48.7	62.7
Total Vulnerabilities (scale of 100)	58.8	49.2	10.6	12.6	49.7	57.9	53.5	18.9	8.4	8.9	6.5
Total Risk (scale of 100)	16.2	18.5	8.4	9.3	34.4	31.4	38.8	19.7	0.0	20.2	19.9

Resiliency Scales (1-100)

Performance Measure	Time Measure	Robustness Measure	Resourcefulness Measure	Recovery Measure
81.3	82.6	56.3	86.8	87.2

Multihazards Interaction Matrix

... will result in this change for other hazards:

a change in:	Blast	CBR	Seismic	Flood	Wind	Fire
a change in Blast	100.0%	16.5%	53.3%	8.8%	48.2%	9.8%
a chang in CBR	10.1%	100.0%	0.0%	0.9%	0.0%	0.0%
a change in Seismic	25.8%	0.0%	100.0%	26.2%	49.4%	3.7%
a change in Flood	5.7%	1.0%	35.4%	100.0%	14.1%	7.0%
a change in Wind	27.3%	0.0%	57.8%	12.2%	100.0%	3.9%
a change in Fire	7.1%	0.0%	5.5%	7.8%	5.1%	100.0%

Total Score Summary
All Scores based on (1-100)

Intrusion:	34.2
Blast (Interior):	44.4
CBR (Interior):	48.8
Blast (Exterior):	35.2
CBR (Exterior):	21.8
Seismic:	17.6
Flood:	9.0
Wind:	36.0
Fire:	19.3
Resiliency:	67.2
Total Risk All Scenarios:	42.6

Print Close

Section 5: Finish the IRVS Process

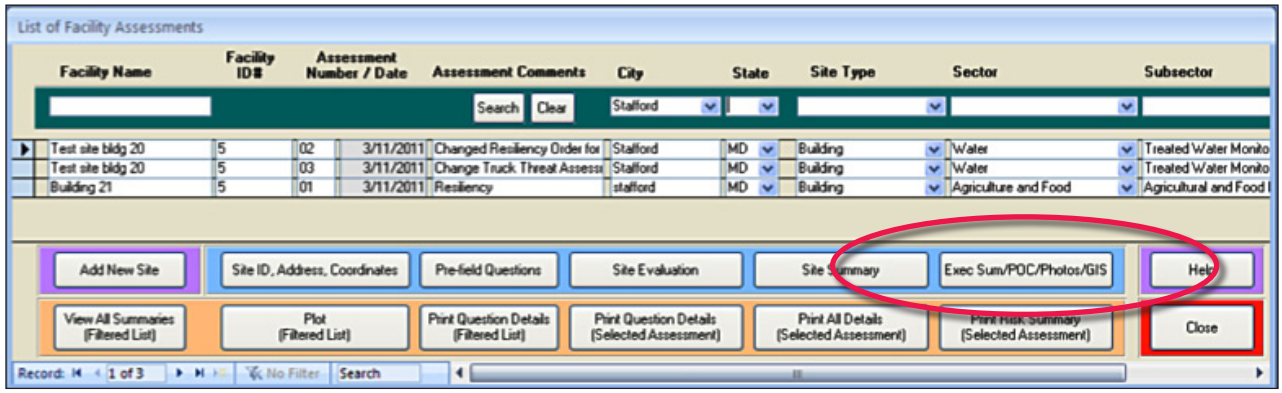
- **Add Executive Summary**
- **Attach Photos, Miscellaneous Files, and Contacts to IRVS Records**
- **Export IRVS Records to Transfer Media**
- **Erase Screening Record from Field Team Database**

During the process, screeners often develop points of contact and collect receive digital files such as drawings, schematics, blueprints, operating procedures, emergency plans, photos of the facility, etc., to assist with their analysis. This optional information as well as an Executive Summary may be added to the database as it provides a baseline for the screening and supports the screener's decisions.

The optional activities available in the database tool include:

- Adding an Executive Summary
- Attaching Photos, Miscellaneous Files, and Contacts to the screening record
- Exporting IRVS records to transfer media
- Empting the Field Team's database

First select one of the screening records by left clicking on the far left column of the **IRVS Record Listing** form. This will mark the screening record desired with a right pointing arrow head if one is not already there. This selects the screening record and links the buttons on the form to that screening record. Next left click the <**Exec Sum/POC/Photos/GIS**> button to open the **Executive Summary/POC/Photos/GIS/Files** form.

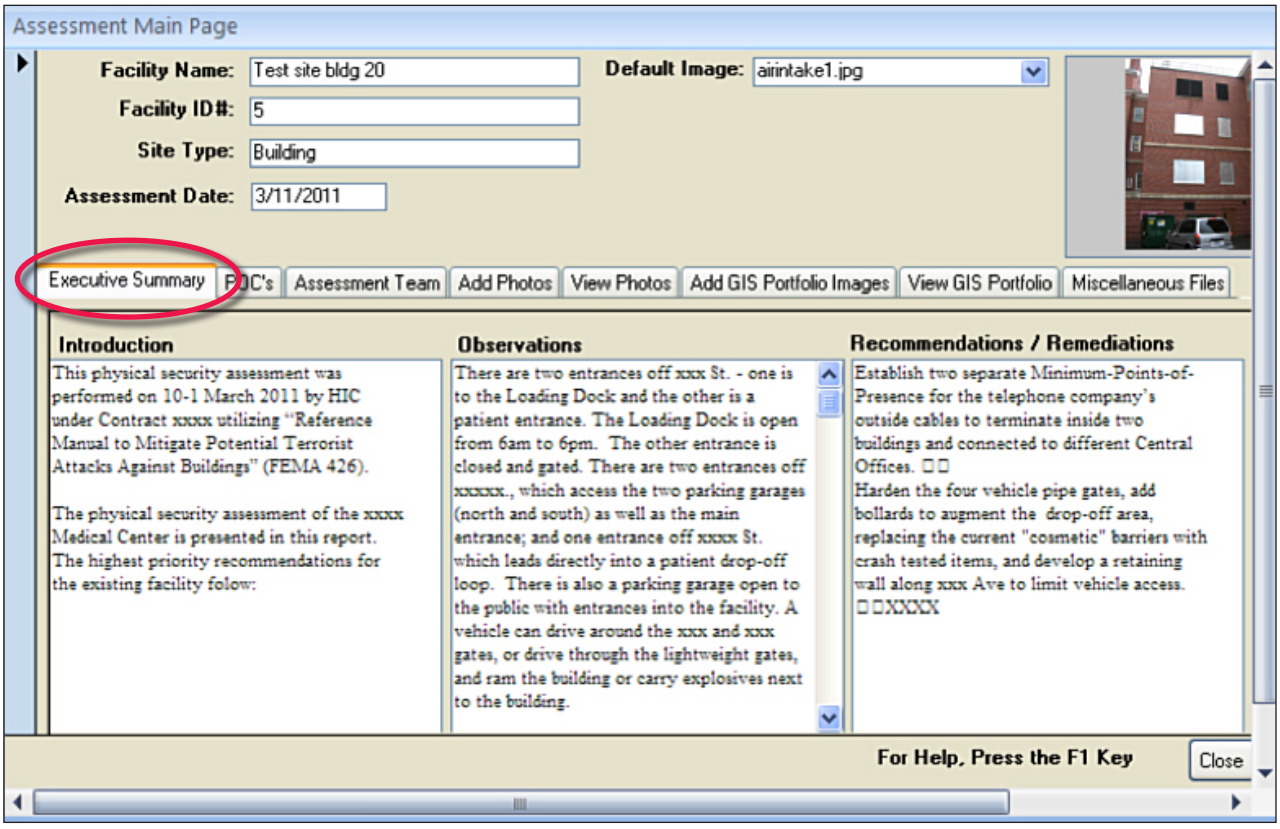


Add Executive Summary

Executive Summary Tab: The Executive Summary Tab of the IRVS database is an area for the screener to write a report on one particular screening record. Left clicking on the <**Executive Summary**> tab will take you to that form.

The Executive Summary form provides three fields to summarize general information about a specific screening record. When printed, these three fields appear as a single document with three main sections: **Introduction**, **Observations**, **Recommendations/Remediation**.

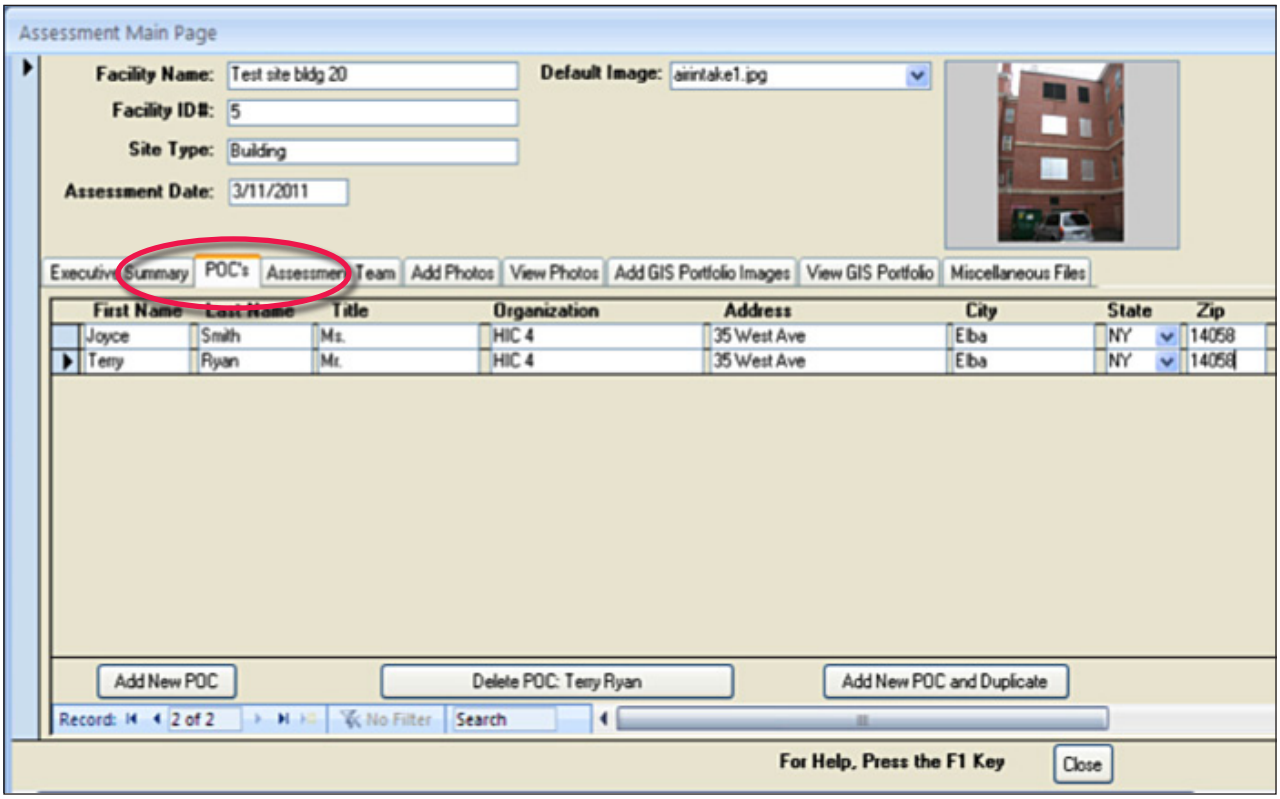
The **Introduction** field usually contains background information, facility location, mission, dates, etc. The **Observations** field might list general information about what was found and particular concerns. Finally, the **Recommendations/Remediations** field is for general recommendations about current conditions.



After loading information, you can left click on <**Close**> to go back to the **IRVS Record Listing** form or left click on a different tab, such as <**Points of Contact**> to directly jump to that function.

Points of Contact

The **Points of Contact** tab takes the screener to the Points of Contact screen for keeping track of the people identified or met during the screening. The buttons across the bottom allow you to add or delete Points of Contact as needed. Add a POC by left clicking on <**Add New POC**>.



This input screen is different than the Screening Team Members input screen, as you enter the information directly in each cell. You can enter the information and move to the next cell by using the <**Tab**> on the keyboard or by left clicking on the cell. Use the slide scale or keyboard arrows to move the screen to see the remaining information on the POC line.

You must press <**Enter**> or the <**Tab**> key after the cells are complete to add the information to the database.

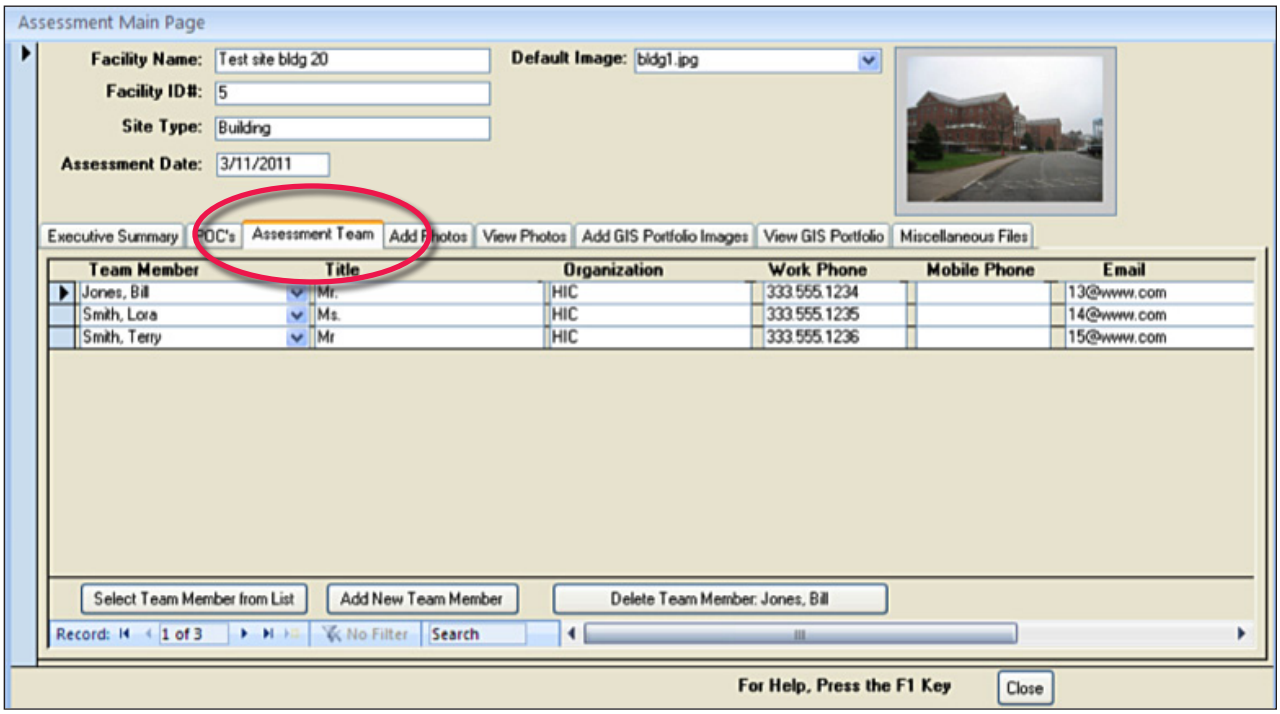
There's even a feature in the POC list to duplicate the address from previous entries, since it is likely that many POCs will have the same business address. Just left click the left column to get the black arrow to appear on the entry with the address to be copied. Then by left clicking on the tab <**Add New POC and Duplicate**> the **Organization**, **Address**, **City**, **State**, and **Zip** blocks will be duplicated on the next entry line.

After loading information, you can left click on <Close> to go back to the **IRVS Record Listing** form or left click on a different tab, such as <**Screening Team>** to directly jump to that function.

Screening Team

CHECK THIS SHOULD BE AN ARROW OR ARE WORDS MISSING?

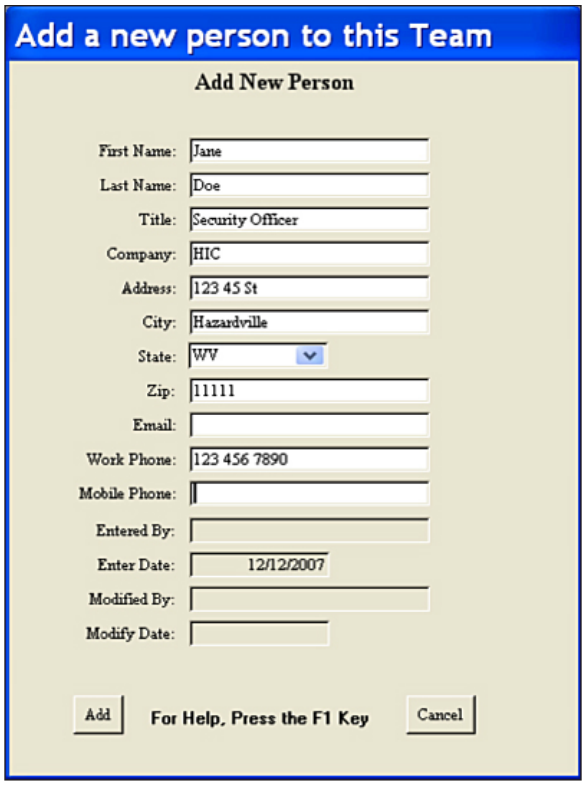
Left clicking on the < displays a form used to track contact information of the screening team members. The buttons across the bottom allow you to add or delete team members as needed.



Left clicking on the <**Add New Team Member**> button takes the assessor to a fill-in-the-blank list. Fill in this screen with as much information as is available or desired.

After adding team member information, left click on the <**Add**> button. You are taken back to the **Screening Team** Tab and you can see the information that was entered. Use the slide scale or keyboard arrows to see the off-screen information. The other buttons allow you to select the Team Member from a List previously generated from other screenings or remove a Team Member from this screening record. Remember to first select one of the screening team members by left clicking on the far left column of the Team Members. This will mark the person desired with a right pointing arrow head if one is not already there.

After loading information, you can left click on <**Close**> to go back to the **IRVS Record Listing** form or left click on a different tab, such as <Add Photos> to directly jump to that function.



Note: After one or more photos are added to the screening record, one may be selected for display on the upper right corner of the form. Simply, left click on the Default Image drop down box, and select the name of the photo to display.

Adding Photos

The **Add Photos**, **Add GIS Portfolio Images** and **Miscellaneous Files** work similarly to add these items to the database and files. A user can browse to a single file and copy it to the database and current screening folder or browse to a file and then copy all files in that folder to the database and current screening folder. A user can also delete files from the database and screening folder.

- First select the <Add Photos> Tab from the **Executive Summary/POC/Photos/GIS/Files** form.
- Next, select either **Copy only the selected image** to attach a single photo, or select **Copy All from the folder** to attach all files in the selected folder.
- Left click the **Browse for a file** button to browse and select a photo to attach.
- A standard browse function screen will open. Search for the file you want, then double click the file or single click the file and single click the Open button to select the file.
- The software confirms that the files were added and attached. Left click Yes to continue with each pop up. Left click **No** or **Cancel** to cancel the attachment.
- Left click OK to return to the **Executive Summary/ POC/ Photos/GIS/ Files** form.
- Left click the **View Photos** tab to ensure the selected photos were added.

Note that the database will recognize any type of file in the "Miscellaneous" folder. However, the database only recognize files with a ".jpg", ".gif" or ".bmp" file extension in the "Photo" and "GIS Portfolio" folders.

A user can also manually add or delete files from the screening subfolders. The database will automatically detect changes and update the current screening's folder when the "Add Photo", "View Photos", "Add GIS Portfolio Images", "View GIS Portfolio" or "Miscellaneous Files" tabs are opened.

Setting the Default Image

After adding photos, the user has an option to select one of the photos as the "Default Image" that will appear on various screens in the top right corner. The image is generally one that represents the location of the screening. For instance, it could be a photo of the building or a sign depicting the name of the facility. Left click on the drop-down menu to the right of the Default Image field and select the desired default image. The image will be present each time the screening is accessed.

Deleting a Photo

To delete a photo, first select the photo from the list by left clicking on the photo's name. This will place a black triangle next to the name of the photo selected.

Next left click on the **Delete Photo** button.

The software confirms the user wants to delete a file. Left click **Yes** to continue with the deletion. Left click **No** or **Cancel** to cancel the deletion.

Viewing Photos

Left click on the **View Photos** tab in the center of the screen to display the photos. You can left click on a photo and enter Photo Zoom which gives a limited capability for viewing the photo in different sizes, using Zoom, Clip, and Internet Explorer. Clip is essentially what you currently see.

If there are more than five items attached to the database, left click the arrow buttons in the lower left corner, to display the additional items. When done, left click Close to exit.

Adding GIS Images

The **Add GIS Portfolio Images**, **Add Photos** and **Miscellaneous Files** functions work similarly to add or delete these items from the database and files. A user can browse to a single file and copy it to the database and current screening folder or browse to a file and then copy all files in that folder to the database and current screening folder. A user can also delete files from the database and screening folder.

- First select the <Add GIS Portfolio Images> Tab from the **Executive Summary/POC/Photos/GIS/Files** form.
- Next, select either **Copy only the selected image** to attach a single GIS portfolio image, or select **Copy All from the folder** to attach all files in the selected folder.
- Left click the **Browse for a file** button to browse and select a GIS portfolio image to attach.
- A standard browse function screen will open. Search for the file you want, then double click the file or single click the file and single click the **Open** button to select the file.
- The software confirms that the files were added and attached. Left click **Yes** to continue with each pop up. Left click **No** or **Cancel** to cancel the attachment.
- Left click on **OK** to finish.
- Left click the View GIS Portfolio tab to ensure the selected photos were added.

Note that the database will recognize any type of file in the "Miscellaneous" folder. However, the database only recognize files with a ".jpg", ".gif" or ".bmp" file extension in the "Photo" and "GIS Portfolio" folders.

A user can also manually add or delete files from the screening subfolders. The database will automatically detect changes and update the current screening's folder when the "Add Photo", "View Photos", "Add GIS Portfolio Images", "View GIS Portfolio" or "Miscellaneous Files" tabs are opened.

Deleting GIS Images

To delete a GIS portfolio image, first select the GIS portfolio image from the list by left clicking on the image's name. This will place a black triangle next to the name of the image selected.

Next left click on the **Delete GIS Portfolio Image** button.

The software confirms the user wants to delete a file. Left click **Yes** to continue with the deletion. Left click **No** or **Cancel** to cancel the deletion.

Viewing GIS Portfolio

Left click on the <**View GIS Portfolio**> tab in the center of the screen to display the GIS portfolio images. You can left click on an image and

enter Photo Zoom which gives a limited capability for viewing the image in different sizes, using Zoom, Clip, and Internet Explorer. Clip is essentially what you currently see.

If there are more than five items attached to the database, left click the arrow buttons in the lower left corner, to display the additional items. When done, left click **Close** to exit.

Adding Miscellaneous Files

The Miscellaneous Files, Add Photos and Add GIS Portfolio Images functions work similarly to add or delete these items from the database and files. A user can browse to a single file and copy it to the database and current screening folder or browse to a file and then copy all files in that folder to the database and current screening folder. A user can also delete files from the database and screening folder.

1. First select <**Miscellaneous Files**> Tab from the **Executive Summary/POC/Photos/GIS/Files** form.
2. Next, select either **Copy only the selected imag**e to attach a single file, or select **Copy All from the folder** to attach all files in the selected folder.
3. Left click the **Browse for a file** button to browse and select a file to attach.
4. A standard browse function screen will open. Search for the file you want, then double click the file or single click the file and single click the **Open** button to select the file.
5. The software confirms that the files were added and attached. Left click **Yes** to continue with each pop up. Left click **No** or **Cancel** to cancel the attachment.
6. Left click on **OK** to finish.
7. Files can then be viewed by double clicking on the File Name.

Note that the database will recognize any type of file in the "Miscellaneous" folder. However, the database only recognize files with a ".jpg", ".gif" or ".bmp" file extension in the "View Photo" and "View GIS Portfolio" folders.

A user can also manually add or delete files from the screening subfolders. The database will automatically detect changes and update the current screening's folder when the "Add Photo", "View Photos", "Add GIS Portfolio Images", "View GIS Portfolio" or "Miscellaneous Files" tabs are opened.

Deleting Miscellaneous Files

To delete a file, first select the file from the list by left clicking on the image's name. This will place a black triangle next to the name of the image selected.

Next left click on the Delete **file** button.

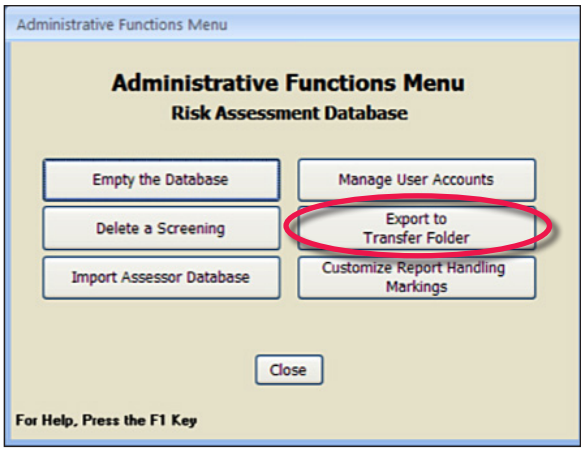
The software confirms the user wants to delete a file. Left click **Yes** to continue with the deletion. Left click **No** or **Cancel** to cancel the deletion.

Export IRVS Records to Transfer Media

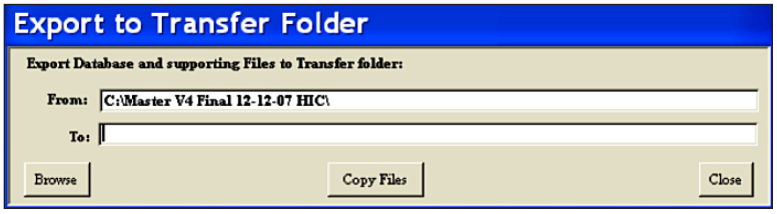
After completing an IRVS screening, the on-site screener usually copies the collected IRVS data from the screeners laptop on to some type of transfer media (USB drive, CD, DVD, etc.) and then loads the data into the organization's Master Database. The screener uses the <Import Assessor Database> and Export to Transfer folder> buttons on the Administrative Functions Menu to transfer the files.

Note: if the screener records the IRVS screening data directly on the organization's Master Database, this step in not needed.

- First the Lead Screener opens his copy of the database to the main menu and left clicks on the <**Administrative Functions**> button to open the Administrative Functions Menu.
- Left click on the <**Export to Transfer Folder**>button.
- This will bring up a window that copies and exports the **IRVS database and screening record folder** (with the associated Photo, GIS files and Miscellaneous subfolders) from the current location to a new location selected by the user.

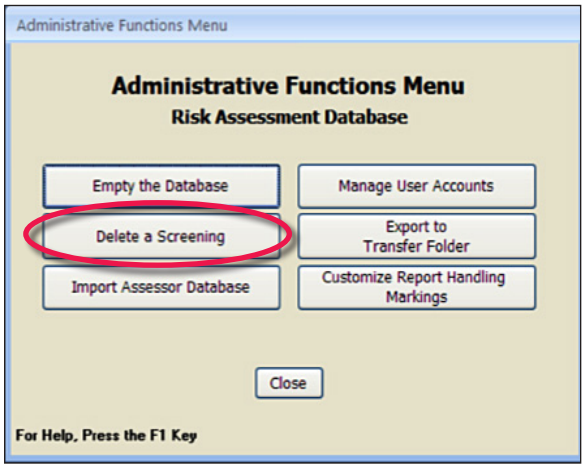


- Use the <**Browse**> button to identify where you want to you want to transfer the files
- Click **Open** to select the folder.
- Then left click **Copy Files**.



- A window will appear asking to confirm that you want to transfer the files. Left click on **Yes**.

- A message will appear indicating that the transfer is complete. Left click on **OK** to return to the **Administrative Functions** Menu.
- The Lead Screener then gives his files on a transfer device to the Master Database operator (usually the IRVS Program Manager). The IRVS Program Manager uses the transfer device (USB drive, CD, DVD, etc.) to copy the screening files to a temporary location on his computer.

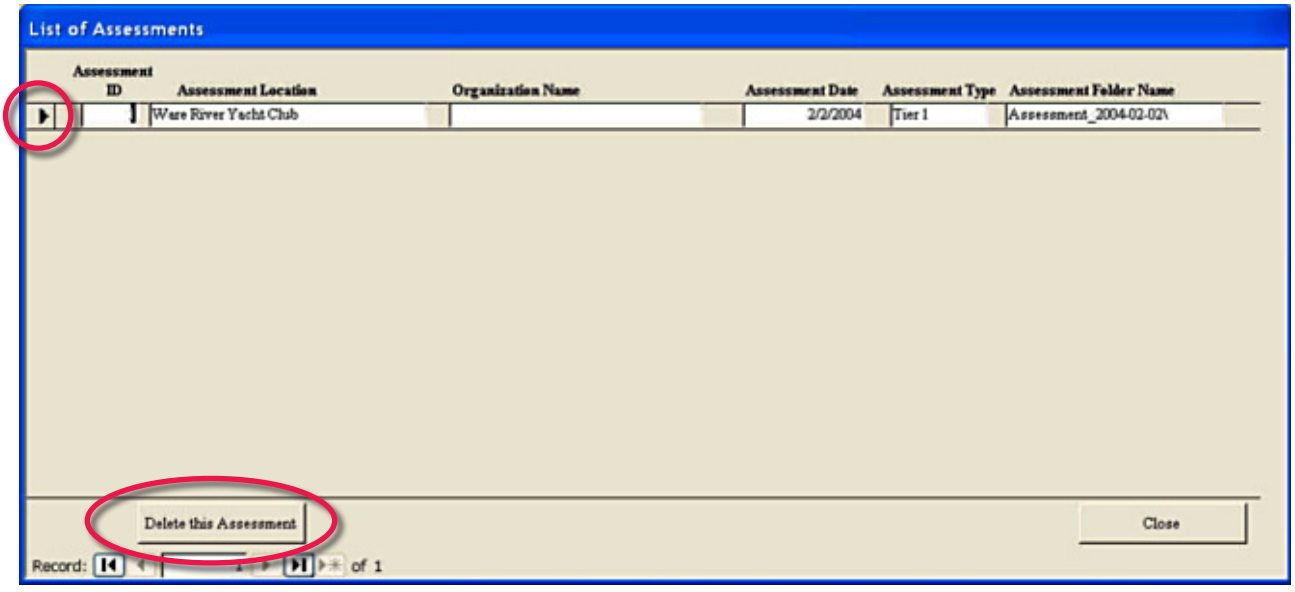


Erase a Screening Record from Field Team Database

Administrators have the ability to erase a single screening record in the database, permanently. This purges the collected data of one single screening record from the laptop. Note data is erased, it cannot be recovered.

- First the Lead Screener opens his copy of the database to the main menu and left clicks on the <**Administrative Functions**> button to open the **Administrative Functions Menu**.
- Left click on the <**Delete a Screening**>button.
- Selecting the <**Delete a Screening Record**> button opens a list of screening records. Select the screening record to erase, then left click <**Delete This Assessment**>. This will open a confirmation window, to ensure you want to permanently erase the selected screening record. Left click on <**Yes**> to **continue** or **cancel**.

Warning: this will erase the screening record from the database, permanently!



Section 6: IRVS Management Processes

- **Create a Filtered Listing of Records**
- **Plot Filtered Listing of Records**
- **Print IRVS Reports**

The primary database at an organization's headquarters, referred to in this guide as the Master Database, is used by managers to store, search print, display and analyze data collected from multiple screenings. Capabilities include:

- Import collected IRVS data from Field Team databases
- Store, search and analyze data on multiple IRVS screenings
- Display and print a variety of reports
- Identify mitigation strategies
- Create a duplicate of an IRVS record for mitigation analysis or "What if" impacts resulting from changes to the Consequence, Threat, Vulnerability and Resiliency status
- Produce standard reports or export report data as a MS Word® or PDF® document for additional editing and formatting
- Export screening risk data to MS Excel® spreadsheets for additional editing and tracking
- Filter and sort screening records by site identification, address, sector and subsector identification, and facility importance
- Plot and display IRVS screening sites and risk values on the users digital mapping program
- Display the Total Risk Summary for one site or for a filtered list of sites.
- Store, display, and print collected digital photos, site plans, floor plans, emergency plans, certain GIS products, and other miscellaneous files collected during screenings
- Perform Database Administrative functions

Create a Filtered Listing of Records

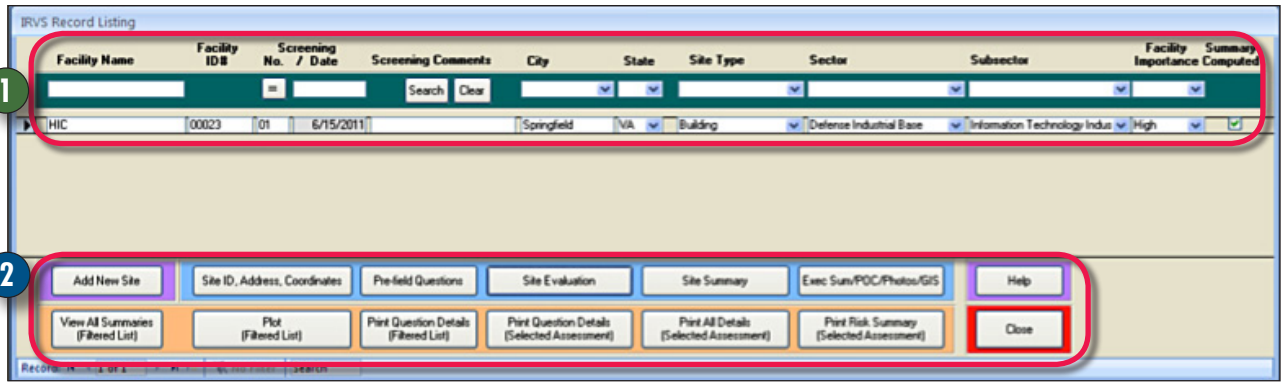
The IRVS Record Listing form displays a list of screening records in the database. The first time you enter the database (with no prior screenings entered), this list will be blank. As screenings are conducted or

transferred into the Master Database, new screening records are added to the bottom of the listing.

The top section of the form (marked with a 1 in the diagram) enables the user to filter the list of records displayed using the fields labeled: **Facility Name**, **Screening Date**, **City**, **State**, **Site Type**, **Sector**, **Subsector**, and **Facility Importance**.

Enter a search term or use the drop down boxes under one or more of the columns to create a query. Then left click the <**Search**> button to filter the records and display a list of only those records that match the query. Left click the <**Clear**> button to clear the query and display all records in the database. Note: for date, use the "<" , ">" or "=" signs to set a range of dates to filter.

After a filtered list of screening records has been produced, use the bottom section of the form (marked with a 2 in the diagram) to display, plot, and print screening details of these screening records.

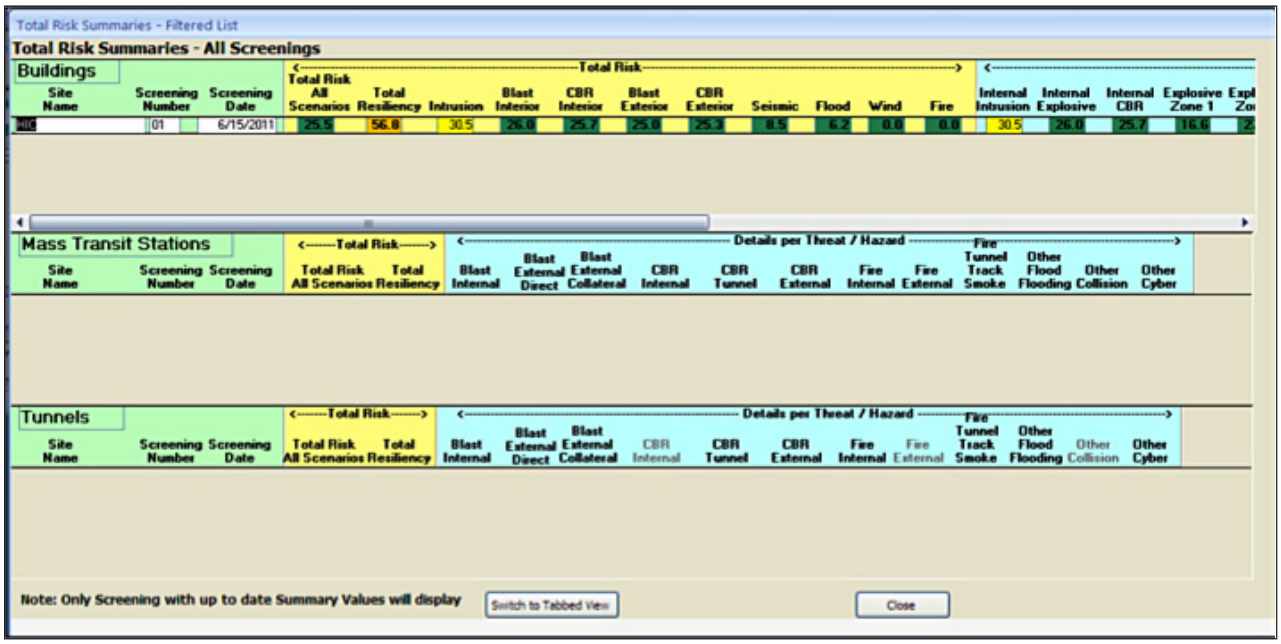


View All Summaries (Filtered List)

After a filtered list of screening records has been produced, left click on the <**View All Summaries** [**Filtered List**]> button to display the **Total Risk Summary – Filtered List** form for only the filtered list of sites.

The **Total Risk Summary – Filtered List** form displays the same information as on a single screening record's Risk and Resiliency Summary form. The Building, Tunnel, and Mass Transit Station summaries can be displayed on three separate Tabs or in a simultaneous view with all values displayed on one form. Use the <**Switch to Tabbed View**> button on the bottom of the form to toggle back and forth between views. Note, in the simultaneous view, the values for the Building screening records are displayed in the top section, the Mass Transit Station values are in the

middle section and the values from Tunnel screenings are on the bottom section. This facilitates comparison and analysis of risk and resiliency values between facilities. (See the catalog for an explanation of the **Risk Summary** values)



Plot Filtered Listing of Records

After a filtered list of screening records has been produced, left click on the <**Plot**> button to display the display IRVS screening sites and risk values on the users digital mapping program .

The button generates a KML file and automatically opens the file for visualization on the users digital mapping program

- The process displays a 100ft, 300ft, and 1,00ft ring around the IRVS site
- The process also displays the following IRVS screening information about the site:

  Name: _____

  Site Type: _____

  Sector: _____

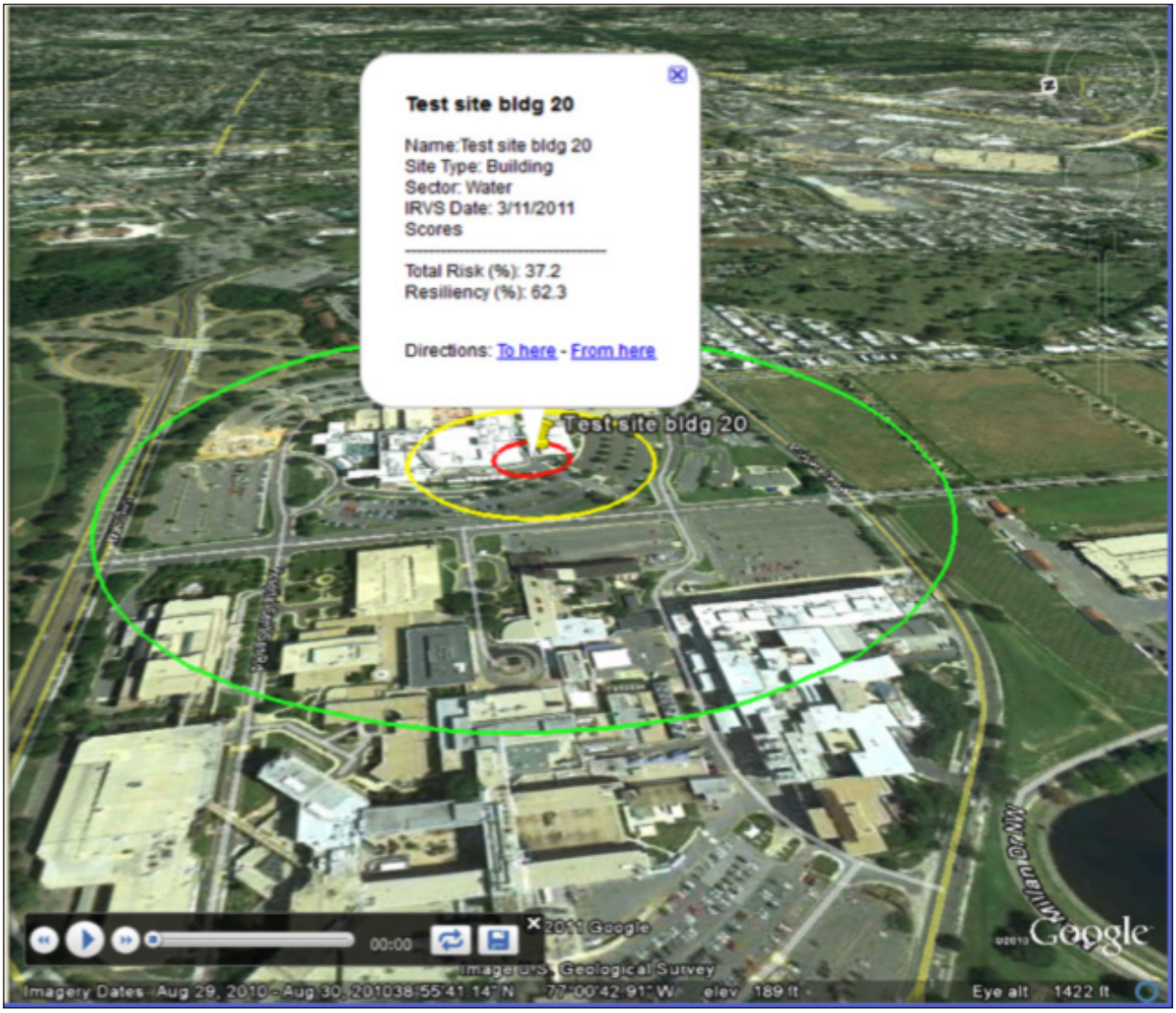
  IRVS Date: _____

  Scores _____

  Total Risk (%):_____

  Resiliency (%): _____

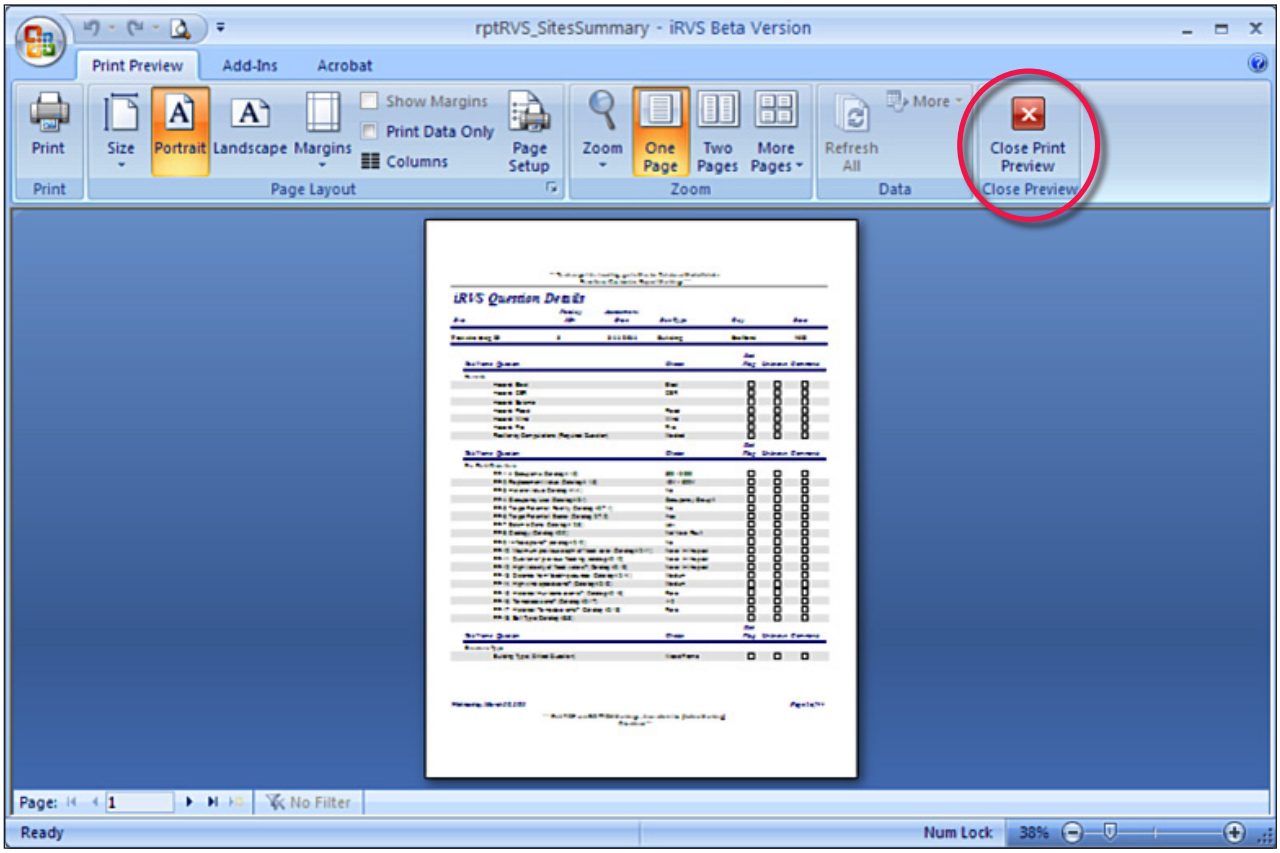
Note: As stated above in the system requirements listing, the database has an optional plotting function to display IRVS site coordinates and screening information on a digital map. The IRVS process can be completed without using this display function. The function requires the use of the computer systems existing mapping program capable of displaying a KML type file, such as Google Earth®. (Keyhole Markup Language (KML) is an XML-based language for defining the display of three-dimensional spatial data in the programs like Google Earth®.)



Print IRVS Reports

The IRVS Record Listing form offers the user four options to produce standard reports or export report data as a MS Word® or PDF® document for additional editing and formatting:

- **Print Question Details** (**Filtered List**): After a filtered list of screening records has been established, the <**Print Question Details**> button opens to a print view screen and displays a long report consisting of the IRVS questions and answers for every screening record displayed on the filtered list. This view does not include the **Risk and Resiliency Summary** screen or the other details of the screening (such as POC listing, Screening Team members, executive summary). Note: When finished printing, use the <**Close Print Preview**> button not the "X" on the upper right corner of the form.
- **Print Question Details** (**Selected Screening Record**) After a single screening record has been selected , the <**Print Question Details** (**Selected Screening Record**)> button opens to a print view screen and displays a report consisting of the IRVS questions and answers for the single screening record selected on the filtered list. This view does not include the **Risk and Resiliency Summary** screen or the other details of the screening (such as POC listing, Screening Team members, executive summary). Note: When finished printing, use the <**Close Print Preview**> button not the "X" on the upper right corner of the form.
- **Print All Details** (**Selected Screening Record**): After a single screening record has been selected , the <**Print All Details** (**Selected Screening Record**)> button opens to a print view screen and displays a report consisting of an expanded amount of IRVS data collected about the single screening record selected on the filtered list. This view does not include the **Risk and Resiliency Summary** screen. Note: When finished printing, use the <Close Print Preview> button not the "X" on the upper right corner of the form.
- **Print Risk Summary** (**Selected Screening Record**): After a single screening record has been selected , the <**Print Risk Summary** (**Selected Screening Record**)> button opens to a print view screen and displays a report consisting of the **Risk and Resiliency Summary** screen. Note: When finished printing, use the <**Close Print Preview**> button not the "X" on the upper right corner of the form.


rptRVS_SitesSummary - iRVS Beta Version
Print Preview
Add-Ins
Acrobat
Print
Size
Portrait
Landscape
Margins
Show Margins
Print Data Only
Columns
Page Setup
Page Layout
Zoom
One Page
Two Pages
More Pages
Zoom
Refresh All
More
Data
Close Print Preview
Close Preview
iRVS Question Details
Page: 1
No Filter
Ready
Num Lock
38%

Section 7: Administrative Functions

- **Empty the Database**
- **Delete a Single Screening Record**
- **Import Field Team Database**
- **Manage User Accounts**
- **Export IRVS Record to Transfer Folder**
- **Customize Report Handling Markings**
- **Change Passwords**

Note: administrative functions are not available to all users. Only those logged on with administrator permission can use the administrative functions menu. For example, only administrators may import field team records into to the Master Database.

Empty the Database

Administrators have the capability to erase all records in a database, permanently. This is only done after transferring your data to a Master Database in a separate computer and when starting a new program. This enables an administrator to remove all database entries and start with an empty database. It also serves to control screening information.

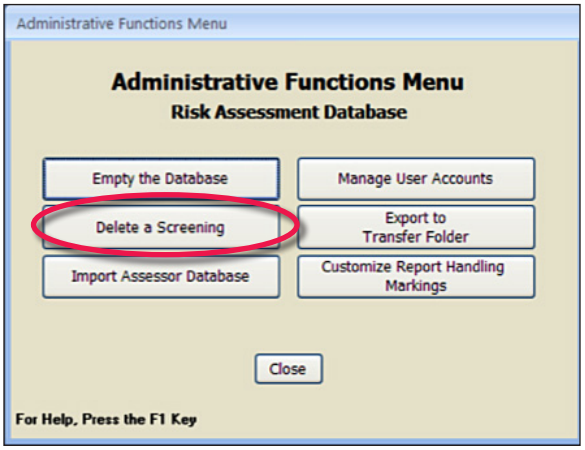
Note: this is permanent. Confirm you have transferred the current information to the Master Database in a separate location before you erase the database.

To empty the database:

1. From the Main Menu, left click on **Empty the Database**.
2. The next window confirms that you want to permanently erase all screening data (not just one screening record, but erase all records). Left click on **Yes** to continue or cancel.
3. You receive a 2nd warning stating that "This action is non-reversible!" Left click on **Yes** to continue or cancel.
4. You receive a final warning asking if you want to delete all files and folders. Left click on **Yes** to continue or **No** to cancel.
5. The files have now been deleted. Left click on **OK** to continue.
6. The next screen that appears during the "Empty the Database" process provides the administrator an option to keep their

customized system defaults or reset the labels to their original listings. Left click on each listed option to reset the labels to their original listings or to keep the administrators customized system defaults.

7. Finalize the process by left clicking on **Continue with these choices**.
8. **Warning: confirm you have transferred the information to the Master Database in a separate computer before you erase the data!**
9. Left click on **OK** to finish. The IRVS database will close. The next time the database is opened, a message will state the configuration table will be re-set. The purged database will have no screening records.



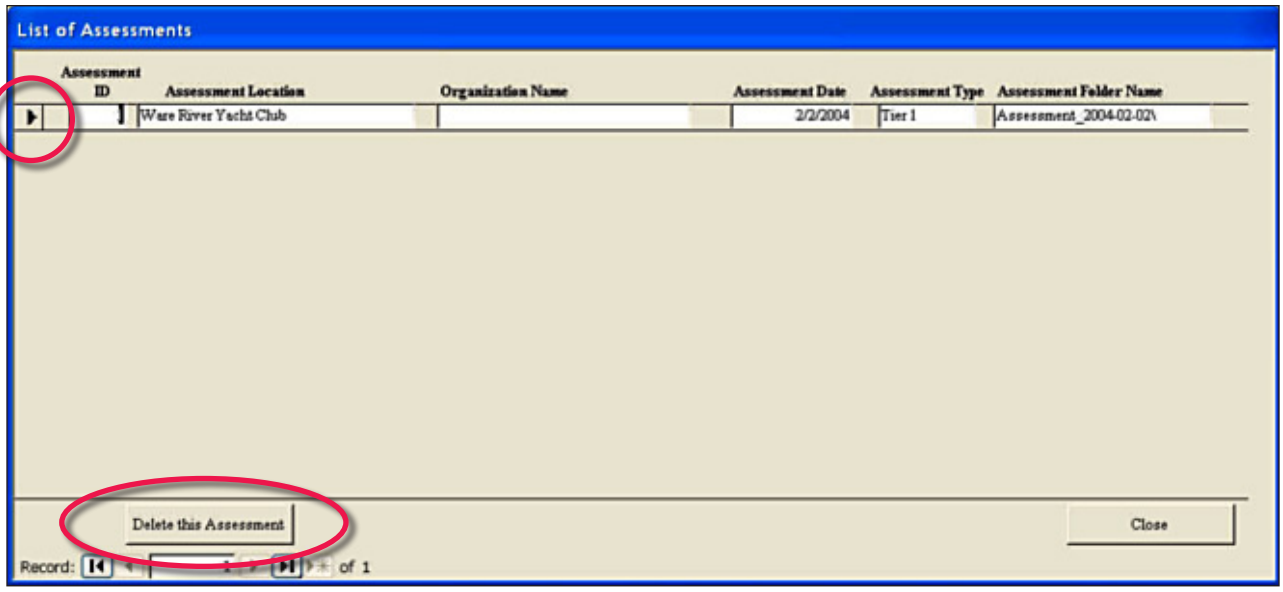
Delete a Single Screening Record

Administrators have the ability to erase a single screening record in the database, permanently. This purges the collected data of one single screening record from the laptop. Note data is erased, it cannot be recovered.

- First open the database to the **Main Menu** form and left click on the <**Administrative Functions**> button to open the **Administrative Functions Menu**.
- Left click on the <**Delete a Screening**>button.

Selecting the <**Delete a Screening Record**> button opens a list of screening records. Select the screening record to erase and then left click <**Delete This Assessment**>. This will open a confirmation window, to ensure you want to permanently erase the selected screening record. Left click on <**Yes**> to continue or cancel.

Warning: this will erase the screening record from the database, permanently!



Import Field Team Database

One of the most important features needed to understand in the **Administrative Functions Menu** is how to import the Field Team database into the Master Database.

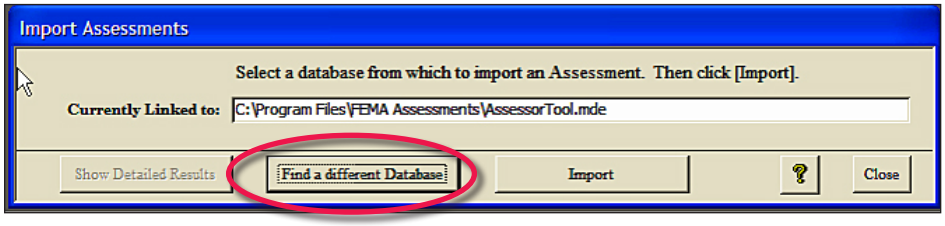
After completing an IRVS screening, the Field Team database from the screeners laptop is copied on to some type of transfer media (USB drive, CD, DVD, etc.) in order to then load the data into the organization's Master Database. The screener uses the <**Export to Transfer folder**> button on the **Administrative Functions** Menu conduct the transfer. (This process was described in Section 6: Finish the IRVS Process, and is repeated in the below paragraph titled: Export IRVS Records to Transfer Media.)

After you have the files transferred you can begin the process to import the Field Team database into the Master Database. Left click on <**Administrative Functions**> button from the **Main Menu**. This brings up the Administrative Functions Menu.

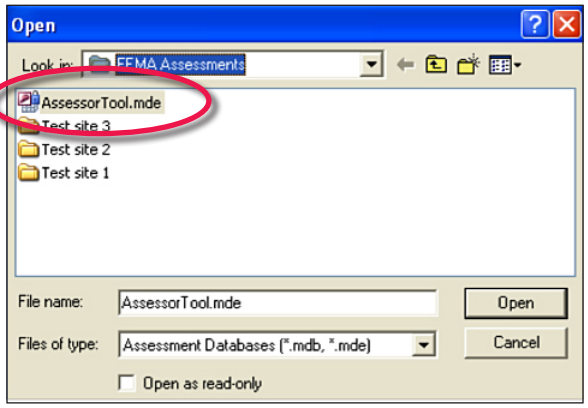
1. The Field Team Screener gives a copy of his IRVS files on a transfer device to the Master Database user (usually the IRVS database Administrator). The IRVS database Administrator uses the transfer device (USB drive, CD, DVD, etc.) to copy the screening files to a temporary location on his computer.
2. The IRVS database Administrator then opens the IRVS Master Database and left clicks on <**Administrative Functions**> button from the **Main Menu**.

3. The Program Manager then left clicks on the <**Import Assessor Database**> button in the middle of the **Administrative Functions** Menu.

4. The next step is to find the IRVS database to import. The below screen opens with the last file identified to which the Master Database was linked.



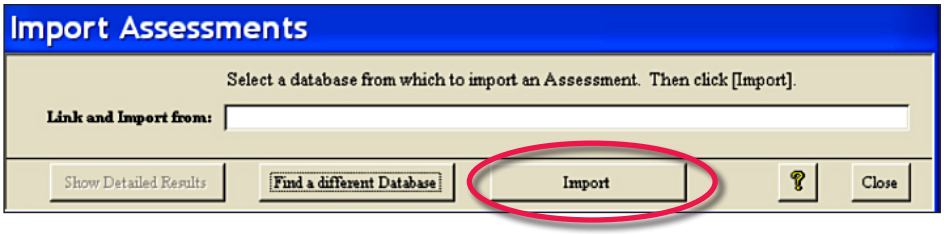
5. Left click on the <**Find a different Database**> button to find the IRVS database that you just transferred to your computer and that you want to import.



6. With this screen you identify the IRVS database that you want to import into the Master Database. Single left click on the file to import, which will put that file into the File Name window and then left click on the <**Open**> button OR double left click on the file to link to this file.

7. Returning to the **Import Assessments** screen the **Link and Import** window now correctly identifies the database to be imported.

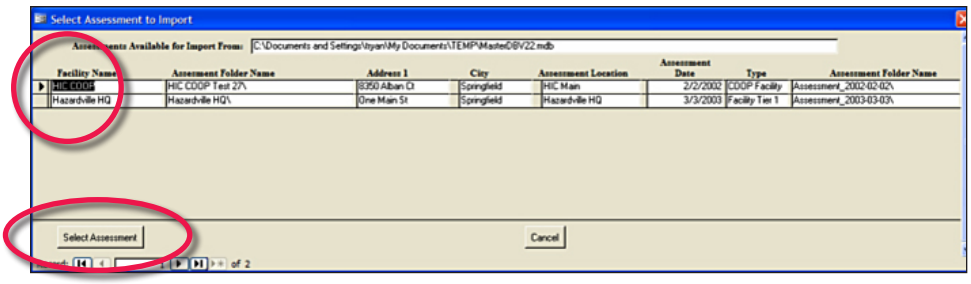
8. Left click the <**Import**> button to initiate the import.



9. A confirmation screen then pops up to ensure this is the desired action for the indicated file. Left click on <**Yes**> to continue.

10. The import function confirms the linking to the desired database has been accomplished. Left click on <**OK**> to continue.

11. A screen opens with a list of facilities that can be imported. Place the arrow on the facility to be imported and left click on <Select Assessment>.



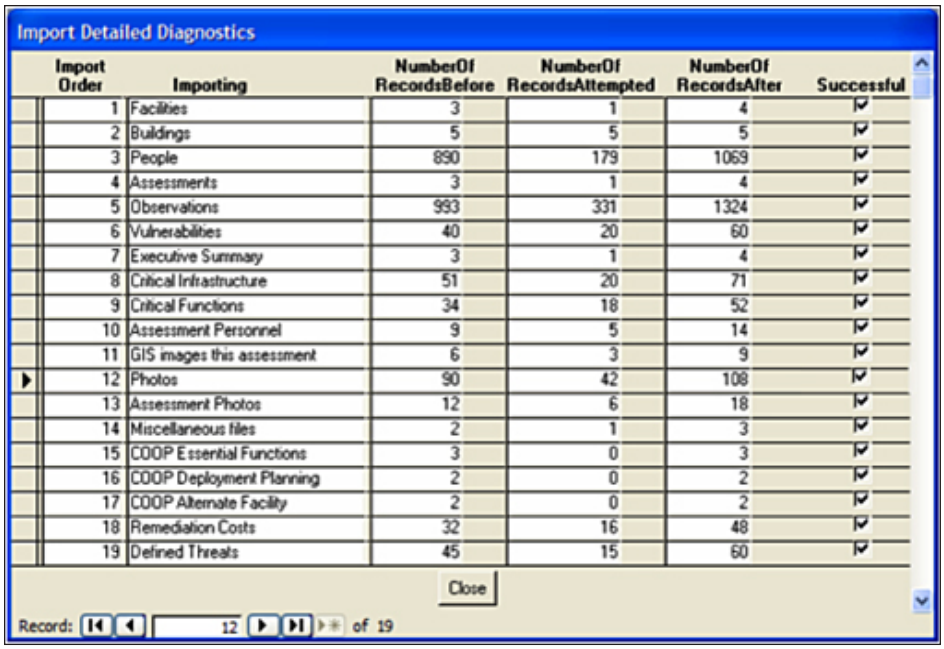
12. The database will then ask if you want to move the supporting files tied to the screening record as well (such as attached photo's). Left click on <**Yes**> to make these transfers. Note: if there are no files in a given folder, the computer will state there are no files to transfer.

13. The final confirmation pop-up you will see will ask if you want to write the files now. Left click <**Yes**> to complete the import process. As in every process, it is always necessary to confirm that what you wanted to have done was actually done.
14. Left click on <**OK**> to finish.
15. After completing the import function, left click on <**Show Detailed Results**> to check that all transfers were successful.

Detailed Diagnostics

The **Import Detailed Diagnostics** screen shows what was in the Master Database before the import, the number of records attempted by the import, and the records after the import. It is recommended to do a quick check by scanning the right hand column, titled Successful, to ensure all boxes are checked.

Another check is to scan Row 4, Assessments. The number of screening records in the Lead Assessor's database being imported should match the number of screening records attempted. Left click on **Close** to close the window and return to the previous screen. This completes the import function.



Import Order	Importing	NumberOf RecordsBefore	NumberOf RecordsAttempted	NumberOf RecordsAfter	Successful
1	Facilities	3	1	4	☑
2	Buildings	5	5	5	☑
3	People	890	179	1069	☑
4	Assessments	3	1	4	☑
5	Observations	993	331	1324	☑
6	Vulnerabilities	40	20	60	☑
7	Executive Summary	3	1	4	☑
8	Critical Infrastructure	51	20	71	☑
9	Critical Functions	34	18	52	☑
10	Assessment Personnel	9	5	14	☑
11	GIS images this assessment	6	3	9	☑
12	Photos	90	42	108	☑
13	Assessment Photos	12	6	18	☑
14	Miscellaneous files	2	1	3	☑
15	COOP Essential Functions	3	0	3	☑
16	COOP Deployment Planning	2	0	2	☑
17	COOP Alternate Facility	2	0	2	☑
18	Remediation Costs	32	16	48	☑
19	Defined Threats	45	15	60	☑

Manage User Accounts

The <**Manage User Accounts**> button enables an administrator to add a new user, delete a user and assign permission levels to users. Reminder: the database is preloaded with the following four users and passwords:

- **Name:** Administrator **Password:** Administrator
- **Name:** Assessor **Password:** Assessor
- **Name:** Editor **Password:** Editor
- **Name:** Reader **Password:** Reader

These passwords are examples only and should be changed after installing the program. Note that the password for the four original users can change, but these four user names cannot be deleted. This is a safety feature to prevent a user from erasing all Administrators from the program.

An Administrator can add a new user, delete a user and assign or change their permission level, referred to as a Group. Select <**Manage User Accounts**> to start the process.

User Groups

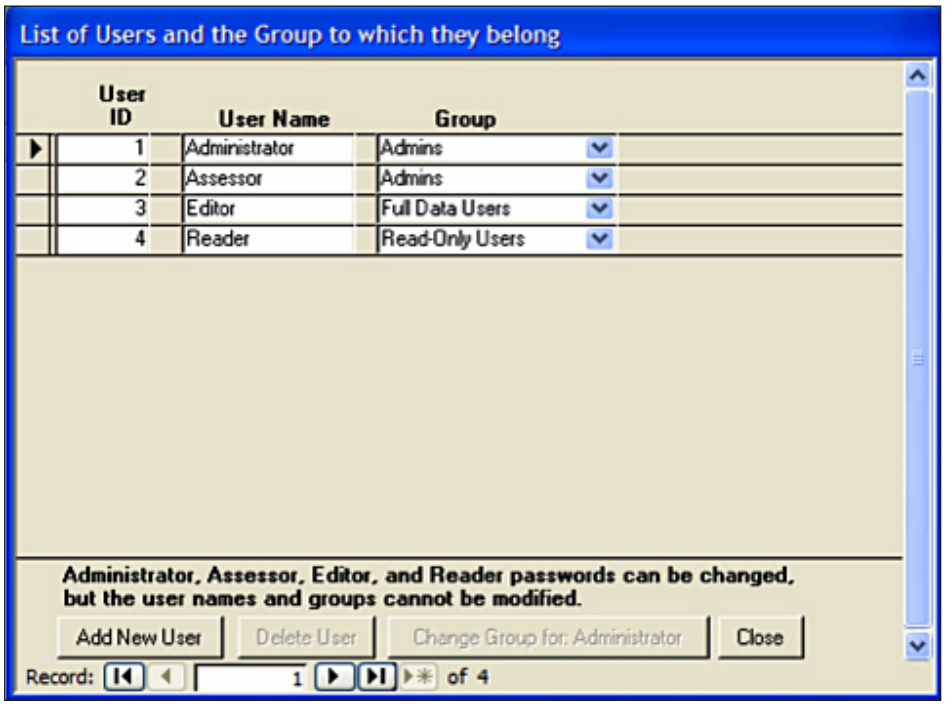
Three user groups have been created for the database in the Workgroup File:

- Admins
- Full Data Users
- Read Only Users

Admins have full access to the database. The **Administrative Functions** button will only be visible for users in the Administrator group. The IRVS database starts with two users in this group, **Administrator** and **Assessor.** They have the initial passwords of "**Administrator**" and "**Assessor**" (Do not include the quotation marks, i.e. " ", in the password.). It is highly recommended to assign them a different password in the Master Database after initial installation.

Full Data Users can view and update data, but not perform administrative functions. The IRVS database starts with one user in this group, **Editor**, which has the initial password of " **Editor** ". (Do not include the quotation marks, i.e. " ", in the password.)

Reader can only view data. The IRVS database starts with one user in this group, **Reader**, which has an initial password of "**Reader**". (Do not include the quotation marks, i.e. " ", in the password.)



Note that the password and permission level for the four original user names can be changed, but these four original user accounts cannot be deleted.

Add a New User

1. From the **Administrative Functions Menu**, left click on **Manage User Accounts**.
2. From the form labeled "List of Users and the Group to which they belong", left click <**Add New User**> button to add a new user name to the database.
3. A screen opens called "**Add a New User Account**". On this screen, type in the new user name.
4. Left click on the downward facing arrow under **Group**.

5. Select from the response field drop down list a users group (permission level).
6. After making entries, left click on the <**Add User**> button to finalize the account.
7. Left click on **OK** to finish.

Delete a User

1. The first step is to select one of the existing users by left clicking on the far left column of the form labeled "List of Users and the Group to which they belong". This will mark the user desired with a right pointing arrow head if one is not already there. This selects the user and links the buttons across the bottom to that user.
2. Next left click on the **Delete User** button to delete a user name from the database.
3. A warning screen opens asking you to confirm the deletion. Left click **Yes** to continue, or **No** or **Cancel** to cancel the action.
4. Left click on **OK** to finish.

Change a User's Group

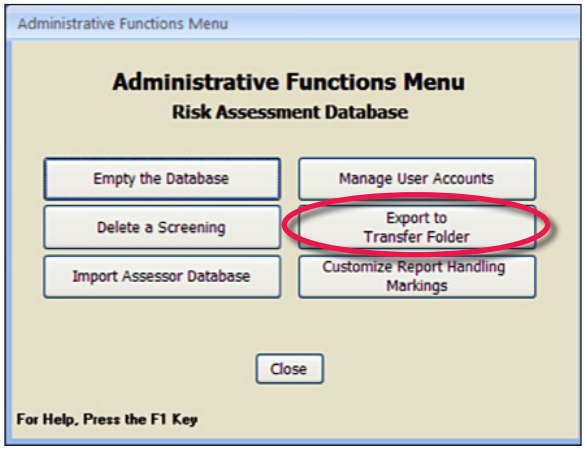
1. The first step is to select one of the existing users by left clicking on the far left column of the form labeled "List of Users and the Group to which they belong". This will mark the user desired with a right pointing arrow head if one is not already there. This selects the user and links the buttons across the bottom to that user.
2. Next left click on the **Change Group for:**… button to change the group of a user from the database. Notice that name of the user selected on the top of the form is displayed in the button **Change Group for:** This is designed to help the Administrator keep track of the account they are working on.
3. A screen opens asking you to select a Group from a drop down Menu. Left click on the downward facing arrow below **Group**.
4. Left click on one of the options from the drop down menu.
5. Left click **Change Group** to continue or **Cancel** to cancel the action.
6. A message appears stating that the user has been removed from the group. Left click on **OK**.
7. A second message appears stating that the user has been now added to the designated group. Left click on **OK** to finish.

Export IRVS Records to Transfer Media

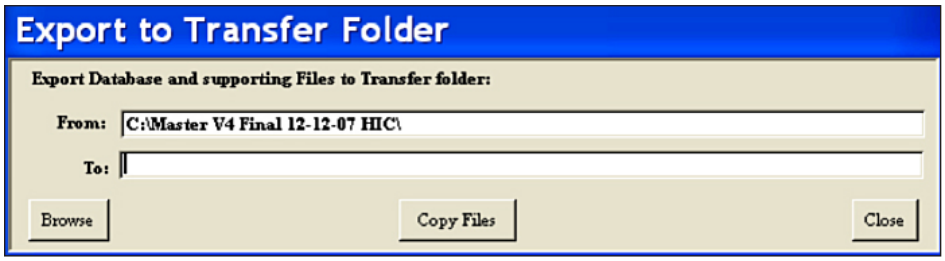
After completing an IRVS screening, the on-site screener usually copies the collected IRVS data from the screeners laptop on to some type of transfer media (USB drive, CD, DVD, etc.) in order to then load the data into the organization's Master Database. The screener uses the <Export to Transfer folder> button on the Administrative Functions Menu to transfer the files.

Note: if the screener records the IRVS screening data directly on the organization's Master Database, this step in not needed.

- First the Lead Screener opens his copy of the database to the main menu and left clicks on the <**Administrative Functions**> button to open the **Administrative Functions Menu**.
- Left click on the <**Export to Transfer Folder**>button.



- This will bring up a window that copies and exports the IRVS database and screening record folder (with the associated Photo, GIS files and Miscellaneous subfolders) from the current location to a new location selected by the user.
- Use the <**Browse**> button to identify where you want to you want to transfer the files
- Click **Open** to select the folder.
- Then left click **Copy Files**.
- A window will appear asking to confirm that you want to transfer the files. Left click on **Yes**.
- A message will appear indicating that the transfer is complete. Left click on **OK** to return to the **Administrative Functions Menu**.
- The Lead Screener then gives his files on a transfer device to the Master Database operator (usually the IRVS Program Manager). The IRVS Program Manager uses the transfer device (USB drive, CD, DVD, etc.) to copy the screening record files to a temporary location on his computer.

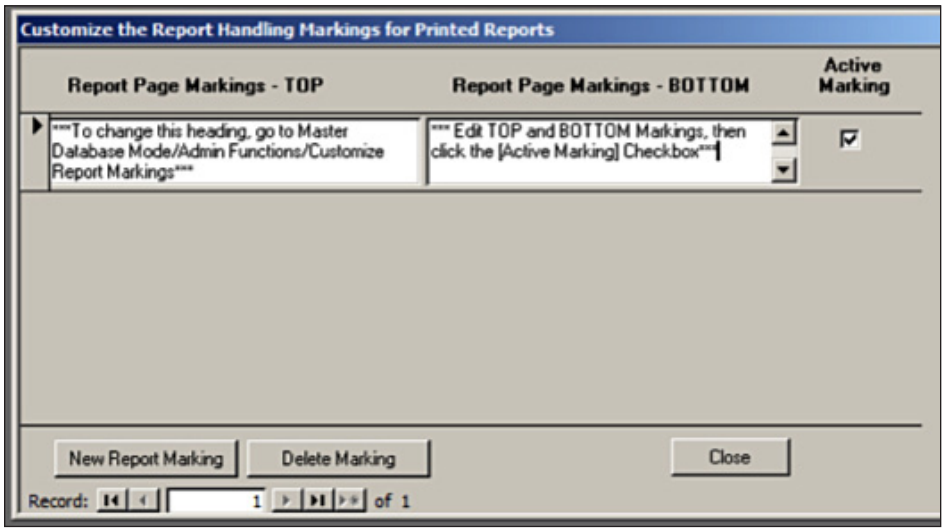


Customize Report Handling Markings

The database administrator can establish customized report handling markings that will be automatically printed on the top and bottom of all reports.

1. Select <**Customize Report Handling Markings**> from the **Administrative Functions Menu**.
2. A screen is opened displaying the "**Report Page Markings - TOP**" entry area on the left and the "**Report Page Markings - BOTTOM**" list on the right. From this form, the system allows administrators to create numerous sets of markings.
3. The default marking can be edited by right clicking in the text box.

4. Additional sets of top and bottom markings can be established by selecting the **New Report Marking** button.
5. Selecting the **Active Marking** checkbox on the far right designates which marking will be used during printing of reports.



Change Passwords

Each user has the ability to change their password associated with their own user name from the Main Menu form. When a user name is initially created by an IRVS Database administrator, the password is blank.

1. To enter the database, simply enter the new user name (assigned by the IRVS Database Administrator), leave the password field blank, and left click **OK**.
2. The program will then force new user to create a password.

It is highly recommended to change all pre-existing passwords for the four pre-established user names at after installing the database (pre-established user names: **Administrator**, **Assessor**, **Editor**, **Reader**). To do this:

1. Log in with each user name
2. From the Main Menu, select **Change Password** which opens the Change Password Form
3. Your user name is pre-populated in the top box
4. Enter your existing password in the **Old Password** box
5. Enter a new password in the **New Password** box

6. Verify your entry by re-typing the new password in the **Verify** box
7. Left click on **Cancel** to cancel
8. Left click **Set Password** to complete the password change
9. Left click on **OK** to finish

Note that passwords must be eight characters long and they must include at least three of the four characters from the following categories:

- Lower case letters (a to z)
- Upper case letters (A to Z)
- Numbers (0 to 9)
- Special characters (`!@#, etc.)

D

Data Collection Form: Paper Version

Pre-Field Information

Complete the information on this page before the field assessment, using additional sheets as needed. The numbers in parentheses refer to the ID number in the catalog. Refer to the catalog for explanations of the information that is requested on this page and the potential sources of the information.

Station name/identification _____

Address/intersection _____

Transit agency _____

Year built _____ Footprint (in square feet) _____

Overview of the station from the transit agency _____

_____

_____

_____

Number of tracks (1.1) _____ Number of levels (1.2) _____

Station elevation (1.3) _____ Replacement value (1.10) _____

Peak daily ridership/transfers (1.4) _____

Terrorist threats against the station (2.3) _____

_____

Terrorist threats against the transit system (2.4) _____

_____

History of flooding affecting the station since opening(2.11) _____

_____

Geology: Soil conditions (3.9) _____

Year(s) of major retrofits (5.3) _____

Retrofit description _____

Operating hours (12.8) _____

Target Density. Number of potential high-value/CIKR targets/buildings within 300 feet and between 300 and 1000 feet of any point of the perimeter of the station (1.7).

CIKR Sector	Within 300 feet	From 300 to 1000 feet
Agriculture and Food		
Banking and Finance		
Chemical		
Commercial Facilities		
Communications		
Critical Manufacturing		
Dams		
Defense Industrial Base		
Emergency Services		
Energy		
Government Facilities		
Healthcare and Public Health		
Information Technology		
National Monuments/Icons		
Nuclear Reactors, Materials, and Waste		
Postal and Shipping		
Transportation Systems		
Water		
TOTAL		

1. Consequences Rating

Characteristic (a)/(f) (b)/(g)			Attribute Options (c)/(h)	(d)/(i)	(e)/(j)			Red Flag	Comments
1.1	Number of Tracks		1	2	3 – 4	5 – 8	> 8		
1.2	Number of Station Levels		1	2	3	> 3			
1.3	Station Elevation		At grade	Above grade	Below grade (above water table)	Above water	Below grade, below water table		
1.4	Peak Number of Riders/Transfers per Day		< 1,000	1,000 – 2,000	2,000 – 5,000	5,000 – 10,000	10,000 – 20,000		
	20,000 – 50,000		50,000 – 100,000	100,000 – 150,000	150,000 – 200,000	> 200,000			
1.5	Station Locality		Remote	Rural	Urban	Dense urban	—		
1.6	Nearby/Adjacent Transportation Systems or Public Assembly Structures Venues		None	Close	Tightly integrated	—	—		
1.7	High-Value Targets/CIKR Targets	**1.7.1** Zone 1: Within 300 feet	None	1 – 6	7 – 12	13 – 19	≥ 20		
		1.7.2 Zone 2: Between 300 and 1000 feet	None	1 – 6	7 –12	13 – 19	≥ 20		
1.8	Impact of Physical Loss/ Criticality	**1.8.1** Station	Local	Regional	National	—	—		
		1.8.2 Track	Local	Regional	National	—	—		
1.9	Social Impact		Low	Moderate	High	—	—		
1.10	Replacement Value (in millions of dollars)		< $1m	$1m – $5m	$5m – $20m	$20m – $50m	$50m – $100m		
	$100m – $200m		$200m – $350m	$350m – $600m	$600m – $900m	> $900m			
1.11	Operational Redundancy		Very high	High	Moderate	Low	Very low		
1.12	Estimated Down Time after a Major Disaster		Very short	Short	Moderate	Long	Very long		

2. Threat Rating

Characteristic (a) (b)			Attribute Options (c)	(d)	(e)			Red Flag	Comments
2.1	Station Locality		Remote	Rural	Urban	Dense urban			
2.2	Peak Number of Riders/Transfers per Day		< 1,000	1,000 – 2,000	2,000 – 5,000	5,000 – 10,000	10,000 – 20,000		
	20,000 – 50,000		50,000 – 100,000	100,000 – 150,000	150,000 – 200,000	> 200,000			
2.3	Terrorist Threat (Credible)	**2.3.1** Station	No	Previous	Current	—	—		
		2.3.2 System	No	Previous	Current	—	—		
2.4	High Value Targets/CIKR Targets	**2.4 1** Zone 1: Within 300 feet	0	1 – 6	7 – 12	13 – 19	> 20		
		2.4.2 Zone 2: Between 300 feet and 1000 feet	0	1 – 6	7 – 12	13 – 19	> 20		
2.5	Significance of Station		Local	Regional	National	International			
2.6	Function Criticality (within System/ Region)		Very low	low	Moderate	High	Very high		
2.7	Number of Entrances/Exits		1 – 2	3 – 4	5 – 8	9 – 12	>12 or unlimited		
2.8	Plaza/Public Area		N/A	None	Well-controlled	Moderate- control	Not- controlled		
2.9	Protective Deterrence Measures		High	Medium	Low	—	—		
2.10	Accessibility of Off-Duty Vehicles/ Equipment		N/A	No accessibility	Low accessibility	Moderate accessibility	High accessibility		
2.11	Flooding History		N/A	None	Limited	Moderate	Severe		

3. Vulnerability Rating: Site

Characteristic (a) (b)			Attribute Options (c)	(d)	(e)			Red Flag	Comments
3.1	Presence of Stand Pipes/Fire Hydrants (Water Supply)		Yes	No	—	—	—		
3.2	Water Drainage		Excellent	Medium	Limited	Deficient	—		
3.3	Natural Barriers		N/A	High	Medium	Low	—		
3.4	Manmade Barriers	**3.4.1** Barriers/ Bollards	N/A	High	Medium	Low	—		
		3.4.2 Fencing	N/A	High	Medium	Low	—		
3.5	Station Elevation		At grade	Above grade	Below grade (above water table)	Above water	Below grade, below water table		
3.6	Depth of Cut and Cover above Station		N/A	Deep	Shallow	Exposed	—		
3.7	Concourse		No	Yes	—	—	—		
3.8	Adjacent buildings		None	Some	Numerous	—	—		
3.9	Geology (Soil Condition)		Hard-rock	Medium	Poor	—	—		
3.10	Accessibility of off-duty vehicles/equipment		N/A	None	Low accessibility	Moderate accessibility	High Accessibility		
3.11	Hazardous Material Storage		No	Yes	—	—	—		

4. Vulnerability Rating: Architectural

Characteristic (a)/(f)		Attribute Options (b)/(g)	(c)/(h)	(d)/(i)	(e)/(j)		Red Flag	Comments
4.1	Number of Entrances	1	2 – 4	≥ 5	—	—		
4.2	Retail Spaces	None	Low	Medium	High	Very high		
4.3	Integrated/Adjacent Parking garages	None	Adjacent parking	Staff only parking	Public parking	—		
4.4	Lobbies (Number and Size)	None	1 small	1 medium	1 large	2 small		
		2 medium	2 large	3+ small	3+ medium	3+ large		
4.5	Number of Observable or Concealed/Not Observable Occupied Spaces	None	No (1 – 2)	No (3+)	Yes (1 – 2)	Yes (3+)		
4.6	Service Entrances	N/A	No	Yes	—	—		
4.7	Crowding/Congestion	Multiple exit types	Escalators only	Stairs only	Elevators only	—		
4.8	Emergency Exits	More than 4	3 – 4	2	1	none		
4.9	Number of Levels	1	2 – 3	More than 3	—	—		
4.10	Ease of Egress from Vehicle/ Trains to Station	Difficult	Moderate	Easy	—	—		
4.11	Plaza/Public Areas	N/A	None	Well-controlled	Moderate Control	Not controlled		

5. Vulnerability Rating: Structural

Characteristic (a)		Attribute Options (b)	(c)	(d)	(e)		Red Flag	Comments
5.1	Liner Relative Thickness	N/A	Thick	Medium	Thin	Very thin		
5.2	Construction material	High strength concrete/steel	Steel/concrete/ prestressed concrete	Wrought iron	Non-reinforced concrete	Masonry or brick		
5.3	Known Retrofits	Yes	No	—	—	—		
5.4	Longest Span	N/A	< 15 feet	25-40 feet	40 – 50 feet	> 50feet		
5.5	Controlling Height	N/A	< 15 feet	25-40 feet	40 – 50 feet	> 50feet		
5.6	Type of Framing	Shell	Plate	Frame	—	—		
5.7	Seismic Design	N/A	Yes	No	—	—		
5.8	Overall Structural Conditions	Excellent	Good	Average	Below average	Poor		

6. Vulnerability Rating: Ventilation Vulnerabilities

Characteristic (a)		Attribute Options (b)	(c)	(d)	(e)		Red Flag	Comments
6.1	Protection of Ventilation Shafts	N/A	Well protected	Somewhat protected	Not protected	—		
6.2	Protection of Ventilation Structures	N/A	Well protected	Somewhat protected	Not protected	—		
6.3	Redundancy of Ventilation Systems	N/A	Yes	No	—	—		
6.4	Ventilation Hardware Exposure	N/A	Hardened enclosure	Covered, not hardened	Visible	—		

7. Vulnerability Rating: Fire Protection System Vulnerabilities

Characteristic (a) (b)			Attribute Options (c)	(d)	(e)			Red Flag	Comments
7.1	Code Inspection		Yes	No	—	—	—		
7.2	Backup Power System		Yes	No	—	—	—		
7.3	Emergency Lighting System		Yes	No	—	—	—		
7.4	Automatic Fire Control Automatic Detection Systems	**7.4.1** Automatic Detection System	Yes	No	—	—	—		
		7.4.2 Fire Control Panel	Yes	No	—	—	—		
		7.4.3 Automatic Detection System Reporting	N/A	Fire department	Off-site control center	Station control panel	No one – local alarm only		
		7.4.4 Activation System	N/A	Release security devices and recall elevators	None	—	—		
7.5	Smoke Dampers in Ventilation System		Yes	No	—	—	—		
7.6	Sprinkler System	**7.6.1** Automatic Sprinkler System	Yes	No	—	—	—		
		7.6.2 Coverage of Automatic Sprinkler System	N/A	Entire station	Partial coverage	—	—		
		7.6.3 Alternate Automatic Extinguishing System	Combination	Clean agent/ water mix	Dry chemical	None	—		
7.7	Station Knox Box		Yes	No	—	—	—		
7.8	Fare Collection System		Open access	Automatic	Restricted turn style	—	—		

8. Vulnerability Rating: Operational Systems

Characteristic (a) (b)			Attribute Options (c)	(d)	(e)			Red Flag	Comments
8.1	Power Supply and Distribution: Enclosures		Well protected	Marginally protected	Not protected	—	—		
8.2	Surveillance and Control	**8.2.1** Coverage of Control Systems	Complete	Partial	None	—	—		
		8.2.2 Quality of Control Systems	High	Medium	Low	—	—		
8.3	Public Address and Communications	**8.3.1** Public Notification (Alerts and Signage for Public Awareness)	Low ridership (see ID I.4)						
			Class 3	Class 2	Class 1	Present – non-operational	None		
			High ridership (see ID I.4)						
			Class 3	Class 2	Class 1	Present – non-operations	None		
		8.3.2 Effectiveness of Public Awareness	High	Moderate	Limited	—	—		
		8.3.3 Asset-related Communications	Low ridership (see ID I.4)						
			Class 3	Class 2	Class 1	Present – non-operational	None		
			High ridership (see ID I.4)						
			Class 3	Class 2	Class 1	Present – non-operational	None		
		8.3.4 Effectiveness of Asset-related Communications	High	Moderate	Limited	—	—		
8.4	Quality of Lighting	**8.4.1** Exterior	High	Medium	Low	—	—		
		8.4.2 Interior	High	Medium	Low	—	—		

9. Vulnerability Rating: Nonstructural Vulnerabilities

Characteristic (a)		Attribute Options (b)	(c)	(d)	(e)		Red Flag	Comments
9.1	Quality of Security Personnel Booths	High	Medium	Low	None	—		
9.2	Fixture Attachments	Secured	Not secured	—	—	—		
9.3	Quality of Barriers/Curbs	High	Medium	Low	None present	—		

10. Vulnerability Rating: Physical Security Vulnerabilities

Characteristic (a) (b)			Attribute Options (c)	(d)	(e)			Red Flag	Comments
10.1	Access Control		Yes	No	—	—	—		
10.2	Intrusion Detection Systems		Yes	No	—	—	—		
10.3	Video and Surveillance Assessment – Monitored CCTV		Yes	No	—	—	—		
10.4	Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE) Detection Equipment		Yes	No	—	—	—		
10.5	Personnel/Baggage CBRNE Screening		Yes	No	—	—	—		
10.6	Vehicular CBRNE Screening		Yes	No	—	—	—		
10.7	Mobile Personnel/Baggage CBRNE Screening		Yes	No	—	—	—		
10.8	Unarmed Guards/Patrol		Yes	No	—	—	—		
10.9	Armed Guards/Patrols		Yes	No	—	—	—		
10.10	Law Enforcement Patrols		Yes	No	—	—	—		
10.11	Asset/Interdiction-related Communications		Yes	No	—	—	—		
10.12	Special Weapons and Tactics (SWAT) Teams		Yes	No	—	—	—		
10.13	Explosion Ordinance Disposal (EDO) Teams		Yes	No	—	—	—		
10.14	Blast Threat: Internal	**10.14.1** Number of Systems	8 or more	4 – 7	1 –3	None	—		
		10.14.2 Overall System Effectiveness	High	Effective	Minimal	Ineffective	No security		

10. Vulnerability Rating: Physical Security Vulnerabilities (cont.)

Characteristic (a) (b)			Attribute Options (c)	(d)	(e)			Red Flag	Comments
10.15	Blast Threat: External (Direct)	**10.15.1** Number of Systems	5 or more	3 – 4	1 – 2	None	—		
		10.15.2 Overall System Effectiveness	High	Effective	Minimal	Ineffective	No security		
10.16	Blast Threat: External (Collateral)	**10.16.1** Number of Systems	5 or more	3 – 4	1 – 2	None	—		
		10.16.2 Overall System Effectiveness	High	Effective	Minimal	Ineffective	No security		
10.17	CBR Threat: Internal	**10.17.1** Number of Systems	5 or more	3 – 4	1 – 2	None	—		
		10.17.2 Overall System Effectiveness	High	Effective	Minimal	Ineffective	No security		
10.18	CBR Threat: Tunnel	**10.18.1** Number of Systems	5 or more	3 – 4	1 – 2	None	—		
		10.18.2 Overall System Effectiveness	High	Effective	Minimal	Ineffective	No security		
10.19	CBR Threat: External	**10.19.1** Number of Systems	5 or more	3 – 4	1 – 2	None	—		
		10.19.2 Overall System Effectiveness	High	Effective	Minimal	Ineffective	No security		
10.20	Fire Threat: Internal	**10.20.1** Number of Systems	5 or more	3 – 4	1 – 2	None	—		
		10.20.2 Overall System Effectiveness	High	Effective	Minimal	Ineffective	No security		
10.21	Fire Threat: External	**10.21.1** Number of Systems	5 or more	3 – 4	1 – 2	None	—		
		10.21.2 Overall System Effectiveness	High	Effective	Minimal	Ineffective	No security		

10. Vulnerability Rating: Physical Security Vulnerabilities (cont.)

Characteristic (a) (b)			Attribute Options (c)	(d)	(e)			Red Flag	Comments
10.22	Fire Threat: Tunnel/ Track/Smoke	**10.22.1** Number of Systems	5 or more	3 – 4	1 – 2	None	—		
		10.22.2 Overall System Effectiveness	High	Effective	Minimal	Ineffective	No security		
10.23	Other Threats: Flood/Flooding	**10.23.1** Number of Systems	5 or more	3 – 4	1 – 2	None	—		
		10.23.2 Overall System Effectiveness	High	Effective	Minimal	Ineffective	No security		
10.24	Other Threats: Collision (Grade/Tunnel/ Elevated)	**10.24.1** Number of Systems	5 or more	3 – 4	1 – 2	None	—		
		10.24.2 Overall System Effectiveness	High	Effective	Minimal	Ineffective	No security		
10.25	Other Threats: Cyber	**10.25.1** Number of Systems	5 or more	3 – 4	1 – 2	None	—		
		10.25.2 Overall System Effectiveness	High	Effective	Minimal	Ineffective	No security		

11. Vulnerability Rating: Cyber Security

Characteristic (a)		Attribute Options (b)	(c)	(d)	(e)		Red Flag	Comments
11.1	Effectiveness of Cyber Security Plan	High	Medium	Low	None	—		
11.2	Effectiveness of Training Programs	High	Medium	Low	None	—		
11.3	Security of Communication, Signal, and Power Systems	Secured	Medium	Low	No security	—		
11.4	Redundancy of Communication Systems	Yes	No	—	—	—		
11.5	Security of Power Supply	Secured	Medium	Low	No security	—		
11.6	Effectiveness of Wireless, Radio, or Satellite Systems During Emergencies	High (regional)	Medium (within jurisdiction)	Low (system only)	—	—		

12. Vulnerability Rating: Organizational Resilience

Characteristic (a)		Attribute Options (b)	(c)	(d)	(e)		Red Flag	Comments
12.1	Emergency Plan	Yes	No	—	—	—		
12.2	Emergency Response Exercises	Full scale	Table top	Workshop	None	—		
12.3	Effectiveness of Emergency Plans	High	Effective	Minimal	Ineffective			
12.4	Security Plan	Yes	No	—	—	—		
12.5	Security Plans Update Status	Within 12 Months	1 – 2 years	2 – 5 years	More than 5 years	None		
12.6	Transit Agency Mass Evacuation Plan	Yes	No	—	—	—		
12.7	Effectiveness of Mass Evacuation Plan	High	Effective	Minimal	Ineffective	—		
12.8	Continuity of Security	No	Yes	—	—	—		
12.9	Report/Exchange Threat Information	Frequent	Seldom/infrequent	None	—	—		
12.10	Training Programs	Well established	Marginal	None	—	—		
12.11	Coordinated Efforts of Local/Regional First Responders	Well established	Marginal	None	—	—		

E

DHS Infrastructure Taxonomy

Infrastructure Taxonomy[1]

This appendix contains an abbreviated version of the Infrastructure Taxonomy prepared by the Department of Homeland Security. It provides a listing of facility types included as part of each of the 18 critical infrastructure categories. Selected facilities provided below focus on facility types that include buildings. This appendix can be used as a reference for tabulating the target density information provided on page 1 of the Data Collection Form).

Agriculture and Food

- Supply
- Processing/Packaging/Production
- Agriculture and Food Product Storage
- Agriculture and Food Product Transportation
- Agriculture and Food Product Distribution
  - Farm Product Wholesalers
  - Grocery and Related Product Wholesalers

1 Source: DHS, 2006, Infrastructure Taxonomy, Version 2, Risk Management Division Office of Infrastructure Protection, Department of Homeland Security, Washington, D.C.

- Food and Beverage Retailers
  - Supermarkets and Grocery Stores
- Food Service and Drinking Facilities
  - Full Service Restaurants
  - Limited Service Food Facilities
  - Drinking Establishments
    - Bars
    - Nightclubs
- Agriculture and Food Supporting Facilities
- Regulatory, Oversight, and Industry Organizations

Banking and Finance

- Banking and Credit
- Securities, Commodities, and Financial Investments
- Insurance Carriers

Chemical

- Chemical Manufacturing Plants
- Hazardous Chemical Transport
- Hazardous Chemical Storage/Stockpile/Utilization/Distribution
- Regulatory, Oversight, and Industry Organizations

Commercial Facilities

- Entertainment and Media Facilities
  - Broadcasting
    - Cable and Other Subscription Programming
    - Radio Broadcasting
    - Television Broadcasting
  - Internet Publishing
  - Motion Picture and Sound Recording Facilities
  - Print Media

- Newspaper and Periodical Publishing
- Other Print Publishing

- Gambling Facilities/Casinos (Resorts)
  - Gambling Cruises Horse and Dog Racetracks
  - Land-Based Casinos
  - Permanently-Moored Casinos
  - Riverboat Casinos
  - Other Gambling Establishments
- Lodging Facilities
  - Bed and Breakfast Inns
  - Hotels and Motels
  - Other Lodging Facilities
- Outdoor Events Facilities
  - Amusement, Theme, and Water Parks
  - Community Parks, Fairgrounds, Pavilions
  - Community Water Facilities
  - Community Special Gatherings
    - Parades
    - Special Events
- Public Assembly/Sports Leagues Facilities
  - Amphitheaters
  - Arenas
  - Convention Centers
  - Golf Courses and Country Clubs
  - Motor Racetracks
  - Movie Theaters
  - Museums, Planetariums
  - Performing Arts Centers and Auditoriums
  - Stadiums
  - Zoos, Aquariums, Botanical Gardens

- Public Assembly/Other Facilities
  - Entertainment Districts
  - Fitness and Recreational Facilities
  - Marinas
  - Skiing Facilities
  - Other Amusement and Recreational Facilities
- Real Estate Facilities
  - Office Buildings
    - Office Buildings – Stand Alone
    - Office Districts
    - Office Parks
  - Residential Units
    - Multi-Family Residences
    - Single-Family Residences
- Retail Facilities
  - Store Retailers
    - Shopping Centers and Malls
    - Shopping Districts
    - Stand-Alone Stores
  - Non-Store Retailers
- Community Organization Facilities
  - Religious Organization Facilities
  - Social Advocacy Organization Facilities
  - Civic and Social Organization Facilities
  - Political Organization Facilities
- Other Commercial Facilities
  - Weather Forecasting Services

Communications

- Wired Communications
- Wireless Communications
- Satellite Communications
- Internet
- Information Services
- Next Generation Networks
- Regulatory, Oversight, and Industry Organizations
- Other Communication Facilities

Critical Manufacturing

- Primary Metal Manufacturing
- Machinery Manufacturing
- Electrical Equipment, Appliance, and Component
- Manufacturing
- Transportation Equipment Manufacturing

Dams

- Dam Projects
- Navigation Locks
- Mine Tailings Dams
- Hurricane Barriers
- River Control Structures
- Levees
- Regulatory, Oversight, and Industry Organizations
- Other Dam Facilities

Defense Industrial Base

- Shipbuilding Industry
- Aircraft Industry

- Missile Industry
- Space Industry
- Combat Vehicle Industry
- Ammunition Industry
- Weapons Industry
- Troop Support Industry
- Information Technology Industry
- Electronics Industry
- Electrical Industry Commodities
- Electronic Industry Commodities
- Mechanical Industry Commodities
- Structural Industry Commodities

Emergency Services

- Law Enforcement
- Fire, Rescue, and Emergency Services
- Search and Rescue
- Emergency Medical Services
- Emergency Management

Energy

- Electricity
- Petroleum
- Natural Gas
- Coal
- Ethanol
- Regulatory, Oversight, and Industry Organizations

Government Facilities

- Personnel-Oriented Government Facilities
  - Personnel-Oriented Buildings and Structures

- Offices and Office Building Complexes
  - Agency Headquarters
  - Field, District and Satellite Offices
  - Legislative Chambers and Offices
  - Judicial Chambers and Offices
  - Data and Call Centers
- Housing
- Correctional Facilities
- Embassies, Consulates, and Border Facilities
- Educational Facilities
  - Pre-Kindergarten
  - Licensed Day Care Facilities
  - K-12 Schools
  - Higher Education Facilities
  - Specialized Education Facilities
- Personnel-Oriented Land

- Service-Oriented Government Facilities
  - Service-Oriented Buildings and Structures
    - Emergency Services
    - Maintenance and Repair Shops
    - Operations, Command, Dispatch, and Control Centers
    - Training Buildings
    - Libraries
  - Service-Oriented Land
- Government Research Facilities
  - Government Research and Development Buildings and Structures
    - Analysis and Assessment Research Facilities
    - Environmental Research
    - Basic Science Research

- Aerospace Research Facilities
- Military Research

- Government Research and Development Land

- Government Storage and Preservation Facilities
  - Storage and Preservation Buildings and Structures
    - Archive and Record Centers
    - Warehouses
    - Weapons and Ammunition Storage
    - Precious Metal Storage
    - Currency Storage
    - Special Nuclear Materials and Waste Storage
  - Storage and Preservation Land
- Government Sensor and Monitoring Systems
  - Global Positioning System
    - Global Positioning System (GPS) Space Segment
    - GPS Control Segment
  - Government Observation Systems
- Government Space Systems
  - Military Facilities
    - Launch Vehicles
    - Launch Facilities
    - Mission Control Facilities
    - Satellites
  - National Aeronatics and Space Admnistration (NASA) Facilities
    - Launch Vehicles
    - Launch Facilities
    - Mission Control Facilities
    - Satellites
  - Military Facilities
    - Army Bases

  - Navy Bases
  - Marine Corps Bases
  - Air Force Bases
  - Coast Guard Bases
  - National Guard Facilities
  - Joint and Combined Military Installations
- Reservations
- Other Government Facilities
- Other Government Buildings and Structures
- Other Government Land

Healthcare and Public Health

- Direct Patient Healthcare
- Public Health Agencies
- Healthcare Educational Facilities
- Health Supporting Facilities
- End-of-Life Facilities
- Regulatory, Oversight, and Industry Organizations

Information Technology

- Hardware Production
- Software Production
- Information Technology Services
- Internet
- Next Generation Networks
- Regulator, Oversight, and Industry Organizations

National Monuments and Icons

- National Monument/Icon Structures
- National Monument/Icon Geographic Areas
- National Monument/Icon Documents and Objects

- Other National Monuments and Icons

Nuclear Reactors, Materials and Waste

- Nuclear Power Plants
- Research, Training, and Test Reactors
- Nuclear Fuel Cycle Facilities
- Radioactive Waste Management
- Nuclear Materials Transport
- Deactivated Nuclear Facilities
- Radioactive Source Production and Distribution Facilities
- Regulatory, Oversight, and Industry Organizations
- Other Nuclear Facilities

Postal and Shipping

- U.S. Postal Service
- Couriers
- Other Postal and Shipping Facilities

Transportation Systems

- Aviation
- Railroad
- Road
- Maritime
- Mass Transit
- Pipelines
- Regulatory, Oversight and Industry Organizations

Water

- Raw Water Supply
- Raw Water Transmission
- Raw Water Storage

- Water Treatment Facilities
- Treated (Finished) Water Storage
- Treated Water Distribution Systems
- Treated Water Monitoring Systems
- Treated Water Distribution Control Centers
- Wastewater Facilities
- Regulatory, Oversight, and Industry Organizations