PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0016 June 2020

Airport Security Vulnerability Assessments

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Mark Crosby
Michael Steinle
Kori Nobel
Theresa Smith
Ross & Baruzzini
St. Louis, Missouri

© 2020 National Safe Skies Alliance, Inc. All rights reserved.

COPYRIGHT INFORMATION

Authors herein are responsible for the authenticity of their materials and for obtaining written permissions from publishers or persons who own the copyright to any previously published or copyrighted material used herein.

National Safe Skies Alliance, Inc. (Safe Skies) grants permission to reproduce material in this publication for classroom and not-for-profit purposes. Permission is given with the understanding that none of the material will be used to imply Safe Skies or Federal Aviation Administration (FAA) endorsement of a particular product, method, or practice. It is expected that those reproducing the material in this document for educational and not-for-profit uses will give appropriate acknowledgment of the source of any reprinted or reproduced material. For other uses of the material, request permission from Safe Skies.

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about their perimeter and access control security.

Through the ASSIST (Airport Security Systems Integrated Support Testing) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying security technologies and procedures.

Through the POST (Performance and Operational System Testing) Program, Safe Skies conducts long-term evaluations of airport-owned equipment to track and document a device or system's performance continuously over its life cycle.

Through PARAS (Program for Applied Research in Airport Security), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee, but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request of proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies PARAS Program Manager*

PARAS 0016 PROJECT PANEL

Sean Bogart *Gresham Smith*
Frank Capello *Broward County Aviation Department*
Sean Cusson *Del Ray Solutions*
Morris McGowan *Partner Forces*
Melissa Osborn *DOWL*
Mike Pilgrim *International Security Concepts*

AUTHOR ACKNOWLEDGMENTS

Ross & Baruzzini would like to acknowledge the assistance of various airports, aviation stakeholders, and representatives from other critical infrastructure sectors in developing this guidance. Special thanks to Shawna Larson, Phoenix International Airport; Andrew Singhas, Savannah International Airport; Kim Dickie, John F. Kennedy International Airport; and Peter L Troyer, Spokane International Airport for reviewing this guidance in draft form.

Richard Albert
ASC, IAH Security
Houston George Bush Intercontinental Airport

Alonzo Baucham
Security Compliance Manager
Dallas-Fort Worth International Airport

Jordan Bauer
Security Manager
Boise Airport

Stacey Black
Senior Security Consultant
Jacobs Engineering

Kim Dickie
Security Manager
John F. Kennedy International Airport

Chuck Farina
Manager
William P. Hobby Airport (HOU)

Rob Forester
Senior Manager, Safety & Security
San Francisco International Airport

Sharon Gordon
Aviation Security
Portland International Airport

Mark Hatfield
Director, Public Safety and Security
Miami International Airport

Jake Hoehn
Airport Security Manager
Minneapolis-St. Paul International Airport

Shawna Larson
Deputy Aviation Director
Phoenix International Airport

Stacey Link
Security Manager
St. Louis International Airport

Robert Lockhart
Deputy Director, Operations
Norman Y. Mineta San Jose International Airport

Douglas Mansel
Manager, Aviation Security
Oakland International Airport

Denise Sines
Security National Practice Lead (Retired)
AECOM

Tim McDonald
Deputy Chief, Airport Security
Detroit Metropolitan Airport

Andrew Singhas
Senior Operations Manager
Savannah International Airport

M. Kevan Smith
Chief, Public Safety
Asheville Regional Airport

Shannon Spence
ESWR Division Deputy Director
Prince William County Service Authority

Adam Steffl
Director, Airport Security
Denver International Airport

Cathryn Stephens
Assistant Airport Director
Eugene Airport

Peter L Troyer
Chief, Airport Police
Spokane International Airport

Renee Tufts
Security Operations Manager
Charlotte Douglas International Airport

CONTENTS

LIST OF TABLES & FIGURES

EXECUTIVE SUMMARY

This guidebook provides airports with a methodology and tools to support planning and conduct of airport-wide Security Vulnerability Assessments (SVA) addressing a broad base of malevolent threats (criminal or terrorist). The methodology can also be used to assess risks stemming from natural hazards and other threats. Tasks conducted to develop this guidebook include:

- Researching and summarizing applicable SVA information inside and outside of the aviation industry
- Developing templates, tools, and checklists to assist airports in conducting assessments
- Identifying and customizing methodologies to rank risks and prioritize security vulnerabilities
- Providing information regarding benefit/cost analysis of mitigation measures
- Providing information to support development of a risk mitigation action plan
- Identifying conditions and considerations that may prompt an update of all or a portion of an SVA

In addition to this guidebook, the research team developed Microsoft Excel-based SVA Tools for use by airport SVA project teams at small, medium, and large hub airports. These are available from Safe Skies upon request.

Planning and conducting SVAs requires resources and can be labor intensive, particularly for broad focused and/or quantitative assessments. However, real and potential benefits to airport management can be gleaned from the SVA process, including:

- **Critical Assets** – Validation of assets most critical to airport operations and other vital functions
- **Hazard/Threat Identification** – Identification and characterization of hazards and threats that convey the greatest potential risk
- **Acceptable Risk** – Evaluation and determination of acceptable risk based on level of impact, legal requirements, or other factors
- **Existing Risk Control Measures** – Identification of risk control measures, which may be insufficient to reduce risk to acceptable levels
- **Physical Security and Technology** – Identification of physical security and technology measures that provide benefit in controlling risk
- **Plans and Procedures** – Identification of planning, procedural, and training needs to reduce risk and support initial phases of a Security Master Plan
- **Fiscal Management** – Effective allocation of fiscal resources to mitigate the threats that convey the highest risk
- **Management Process** – Development of a planned, ongoing cycle to evaluate and mitigate risk and evaluate mitigation measures
- **Stakeholder Coordination** – Relationship building, development of consensus regarding risks, and responsibility sharing among airport stakeholders.

Based on a review of methodologies used in other sectors and assessment of stakeholder feedback, a recommended eight-step SVA methodology for airports is summarized below:

1. **Project Charter** – Define scope, team, schedule, budget/resources, and goals. Understanding how to get started with an airport SVA requires a plan. A project charter is provided, which allows development of a scope, project team, schedule, and budget, as well as identification of other SVA requirements (see Section 4.1 and Appendix C, Table C-1).

2. **Asset Characterization** – Identify assets that, if compromised by a threat, could result in interruption of service, functional degradation, or other impacts. The SVA process focuses on critical assets and specific threats to which those assets may be susceptible. Reference assets for airports were developed as a starting point for SVA project teams. While the references provide well-researched assets and threats, SVA project teams should customize the assets for their specific airport (see Section 4.2 and Appendix C, Tables C-2 and C-3).
3. **Threat Characterization** – Identify plausible threat scenarios and potential impacts. Reference threats for airports were developed as a starting point for SVA project teams. While the references provide well-researched assets and threats, SVA project teams should customize the threats for their specific airport (see Section 4.3 and Appendix C, Tables C-4 and C-5).
4. **Consequence Analysis** – Quantify impacts of threat scenarios based on the potential for fatalities, injuries, displacement/workaround, replacement/repair, and loss of service costs. Of the three factors that define risks associated with asset-threat combinations, consequence analysis is the most data intensive. Factors that can be used to support consequence analysis are provided in Section 4.4 and Appendix C, Table C-7 (also see the SVA Tools, Tabs 4.1–4.3).
5. **Probability Analysis** – Estimate the likelihood of threats occurring based on intelligence, historical data, estimates of the asset's attractiveness to a perpetrator, and ease of occurrence. Tools to support probability analysis are described in Section 4.5 (also provided in Tabs 5.1 – Probability Outsider and 5.2 – Probability Insider in the SVA Tools).
6. **Vulnerability Analysis** – Identify conditions that can be exploited to commit a malevolent act, including asset characteristics, technology, and operational practices. Tools to support vulnerability analysis are described in Section 4.6 (also provided in Tabs 6.1 – Vulnerability-Outsider and 6.2 – Vulnerability-Insider in the SVA Tools).
7. **Risk Analysis** – Calculate risk (*Risk = Consequence x Probability x Vulnerability*) and rank asset-threat combinations relative to their specific levels of risk.
8. **Risk Management** – Determine which asset-threat combinations should be prioritized for mitigation based on risk ranking, identify acceptable levels risk, assess and implement mitigation options, periodically evaluate mitigation measures, and conduct periodic re-assessment of risk. Recommendations for risk ranking and risk management are provided in Sections 4.7 and 4.8.

The methodology described within this guidebook addresses both quantitative and qualitative risk assessment. Quantitative assessment of risk is labor intensive and requires substantial data that may be difficult to obtain. Certain data points, for example, are premised on human factors, which are difficult to determine with a high degree of confidence. Cost data for consequence analysis may also be difficult to identify. If resources or data are lacking, qualitative risk assessment provides a legitimate alternative to quantitative risk assessment. While results may lack the acuity of quantiative risk assessment, qualitative risk assessment is a cost-effective alternative and may provide a more realistic approach, particularly for in-house airport SVA project teams. The benefits of quantitative and qualitative risk assessments are discussed specifically in Section 1.2 and throughout Section 4.

Following completion of the SVA, security mitigation action planning and benefit/cost analysis can be used to support evaluation and implementation of mitigation options. A security mitigation action plan can be developed and generally includes:

- Identifying countermeasure or mitigation options
- Estimating the efficacy of mitigation options in reducing risks for specific asset-threat combinations
- Developing Scope of Work for each option
- Estimating costs of each option

Information regarding standards and methods for developing mitigation options is provided in Section 5.

As a final step to support management decisions regarding mitigation, benefit/cost analysis, described in Section 6, can be performed using the potential monetary benefits and the project costs associated with the mitigation measure. Benefit/cost analysis enables comparison of multiple mitigation measures to identify the most cost-effective strategy.

Research data used to develop this guidebook is provided in Appendices A–C. These appendices catalog data from airport and other critical infrastructure literature, government doctrine, and interviews conducted during the project to support processes recommended throughout the guidebook. In addition to providing data regarding development of this guidebook, the literature review (Appendix B) provides information that may be useful to those who have not conducted SVAs.

SVAs can be challenging and resource-intensive. However, airport management can benefit greatly from SVAs in identifying threats, vulnerabilities, and risks to support informed decision-making and to prioritize limited resources.

PARAS ACRONYMS

ACRP	Airport Cooperative Research Project
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CEO	Chief Executive Office
CFR	Code of Federal Regulations
COO	Chief Operating Officer
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IP	Internet Protocol
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

ACC	American Chemistry Council
ANSI	American National Standards Institute
AOC	Airport Operations Center
API	American Petroleum Institute
ASME	American Society of Mechanical Engineers
AWWA	American Water Works Association
BCA	Benefit/Cost Analysis
BCR	Benefit/Cost Ratio
CBR	Chemical, Biological, and Radiological
CIP	Critical Infrastructure Protection
CPG	Comprehensive Preparedness Guide
CPI	Consumer Price Index
CSO	Chief Security Officer
DOT	Department of Transportation
EOC	Emergency Operations Center
ERM	Enterprise Risk Management
FSL	Facility Security Level
FTA	Federal Transit Administration
FV	Future Value
HAZUS	Hazards US (FEMA geographic information system-based natural hazard analysis tool)
HSEEP	Homeland Security Exercise and Evaluation Program
HVAC	Heating, Ventilation, Air Conditioning
ICAO	International Civil Aviation Organization
JVA	Joint Vulnerability Assessment
MEP	Mechanical, Electrical, Plumbing
MS	Military Standard

NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NPG	National Preparedness Goal
NPSTC	National Public Safety Telecommunications Council
NPV	Net Present Value
PAP	Physical Asset Protection
PASNF	Public Area Security National Framework
PBIED	Person-Borne Improvised Explosive Device
PDC	Protective Design Center
PSIM	Physical Security Information Management (System)
RAM	Risk Assessment Methodologies
RCA	Root Cause Analysis
ROM	Rough Order of Magnitude
SAFETY Act	Support Anti-Terrorism by Fostering Effective Technology Act of 2002
SCIF	Sensitive Compartmented Information Facilities
SME	Subject Matter Expert
SOCMA	Synthetic Organic Chemical Manufacturers Association
SOW	Scope of Work
SVA	Security Vulnerability Assessment
THIRA	Threat and Hazard Identification and Risk Assessment
VBIED	Vehicle-Borne Improvised Explosive Device

SECTION 1: INTRODUCTION

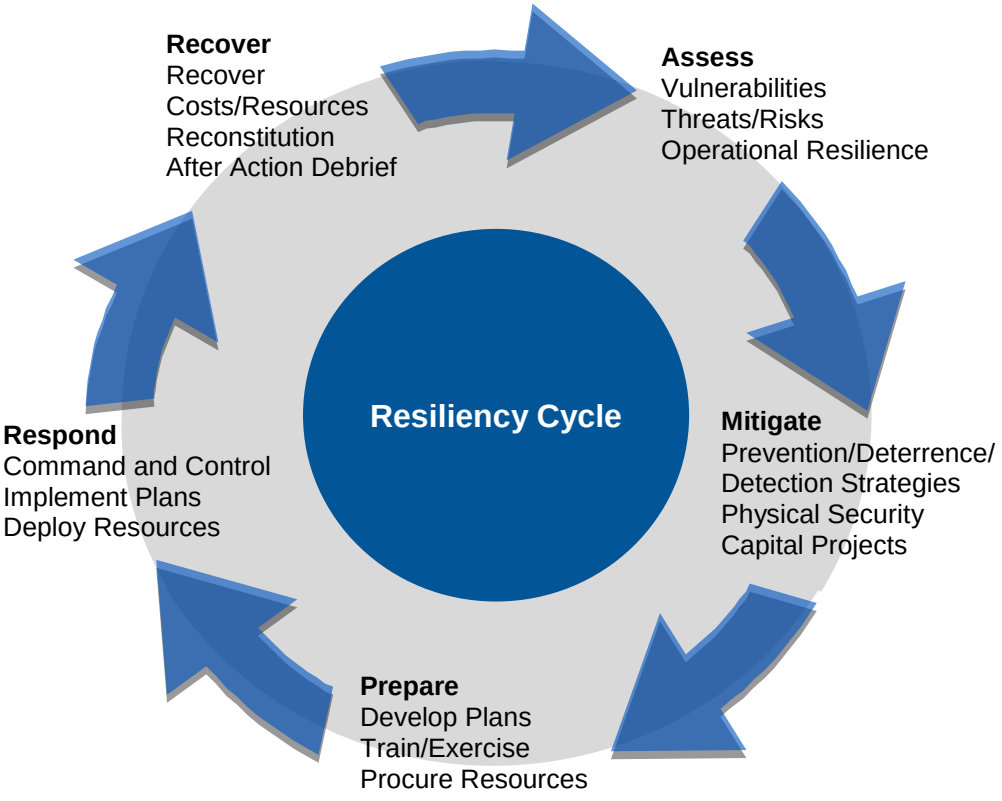
Ross & Baruzzini conducted research on behalf of Safe Skies to provide airport-specific guidance regarding planning and execution of Security Vulnerability Assessments (SVA). While many airports currently conduct SVAs and update them periodically to address security mitigation needs, airport-specific information regarding SVAs is currently limited. The research and this resulting guidebook are intended to support airport management in conducting efficient, effective, and relevant SVAs.

1.1 The Importance of SVAs to Mitigate Risk

Identifying and mitigating security gaps is critical to protecting airports from malevolent threats. However, the SVA and mitigation process is often overlooked as a critical component of an effective security program. Research also indicates that a specific framework for conducting SVAs at airports is lacking compared to other critical infrastructure sectors.

It is important to implement a proactive and ongoing SVA and mitigation process before disaster strikes. As characterized in Figure 1-1, assessing threats and vulnerabilities to which an airport may be susceptible is the first step in the cycle to reduce risk and foster resiliency, and understand the airport's security posture and potential mitigation needs.

Figure 1-1. The Resiliency Cycle



An ongoing SVA and mitigation process allows airports to address a broad base of threats and hazards or focus specifically on security vulnerabilities, as needed. A flexible process allows airports to adjust to evolving threats, is amenable to non-traditional threats, and allows implementation of risk-based mitigation measures to protect people, processes, and infrastructure. This guidebook provides a comprehensive approach to assessing airport security risks, provides tips on conducting less-intensive qualitative analysis, and provides a structure to address other risks, including cyber threats and natural hazards.

As with any methodology, some SVA steps require judgment on the part of the assessors and are susceptible to subjectivity. The value of performing an SVA is not derived from the precision of certain factors (such as probability), but rather from identifying legitimate asset vulnerabilities and threats to the

airport mission and, subsequently, mitigation measures. In short, the SVA process can be described as equal parts art and science.

1.2 Quantitative vs. Qualitative Assessment

Quantitative assessment of risk is labor intensive and requires substantial research and experiential data, which may be difficult to collect and may not provide a high degree of accuracy. For example, the probability of a specific type of incident occurring is premised on human factors, which are difficult to determine with a high degree of confidence. However, quantitative assessment can provide information to support identification of costs associated with risks and mitigation measures and, ultimately, can support more informed risk management decisions using benefit/cost analysis, if desired.

Data used to identify probability and vulnerability is often difficult to obtain and subjective. When resources and data for quantitative assessment are lacking, qualitative assessment may be a legitimate alternative. Qualitative risk assessment uses a relative or descriptive scale to measure probability of occurrence, such as a scale of low-medium-high, whereas quantitative assessment identifies probability of each risk as a percent. Examples of qualitative matrices for probability and consequence are provided in Tables 1-1 and 1-2.

Table 1-1. Qualitative Probability Matrix

Rating	Probability	Condition
1	Near Zero	Highly unlikely to occur and requires exceptional circumstances.
2	Low	Not likely to occur. Requires specific conditions.
3	Moderate	Occurrence is possible, but difficult to predict.
4	High	Likely to occur. Risk has occurred under similar conditions.
5	Near Certain	Probability of occurrence near certain. Conditions favorable for risk to occur.

Table 1-2. Qualitative Consequence Matrix

Rating	Consequence	Social Cost (casualties)	Physical Cost (damage to assets)	Overall Monetary Cost
1	Very Low	No casualties	None	None
2	Low	1– 5	<$1,000	<$100,000
3	Moderate	6–10	$1,001 – $10,000	$100,001 – $1,000,000
4	High	11–20	$10,001 – $100,000	$1,000,001 – $5,000,000
5	Very High	>20	>$100,000	>$5,000,000

Using the qualitative matrices above, a qualitative risk matrix or heat map can be used to rate risk levels for each asset-threat combination, as shown in Figure 1-2.

Figure 1-2. Heat Map for Qualitative Consideration of Probability and Impact

Probability ↑ / Impact →	Little to No Impact	Low Impact	Moderate Impact	High Impact	Catastrophic Impact
Near Certain	No action necessary	Consider mitigation	Consider mitigation	Mitigation recommended	Mitigation recommended
High	No action necessary	Consider mitigation	Consider mitigation	Mitigation recommended	Mitigation recommended
Moderate	No action necessary	No action necessary	Consider mitigation	Consider mitigation	Mitigation recommended
Low	No action necessary	No action necessary	Consider mitigation	Consider mitigation	Mitigation recommended
Near Zero	No action necessary	No action necessary	No action necessary	Consider mitigation	Consider mitigation

Qualitative assessment is a cost-effective alternative to quantitative assessment; however, the values are more subjective and benefit/cost analysis is performed using notional monetary estimates of impact. Other differences are indicated in Table 1-3.

Table 1-3. Qualitative vs. Quantitative Risk Assessment

Qualitative Risk Assessment	Quantitative Risk Assessment
Generally performed with fewer resources and a small number of personnel	Requires a diverse team of subject matter experts (SME) and is resource intensive
Considers all risks in a more general and subjective manner	Consider all risks initially, but eliminates certain risks based on quantified measures indicating low probability, low vulnerability, and/or low consequences
Risk is not analyzed mathematically to identify probability but uses stakeholder input to establish subjective measures of probability and impact	Uses probability distributions to characterize probability and consequences via mathematical calculations and/or simulation tools
Assigns numeric rankings of probability and impact based on stakeholder input	Predicts consequences in monetary terms, establishes probability of threat, and estimates vulnerability of assets to determine overall risk

Qualitative risk assessment provides a legitimate alternative to quantitative risk assessment when available team members, resources, and time are lacking. While results may lack the acuity of quantiative risk assessment, qualitative risk assessment is a cost-effective alternative.

1.3 Application of the Guidebook

Although not every consideration discussed herein is applicable to every airport, the guidebook is designed to assist airports of all sizes in evaluating risks that are relevant to their location.

The methodologies described in this guidebook are applicable to ongoing operations and periodic evaluation of risk, and can also be used before the start of any new capital projects to identify critical assets, potential threats and hazards, and mitigation strategies to consider during design and construction. When applied to new capital projects, risks, vulnerabilities, threats, and hazards should be used to develop design guidance criteria and in the RFP phase.

To support SVA planning and conduct, SVA Tools for small, medium, and large hub airports have been developed and are available from Safe Skies upon request. The Tools are discussed in conjunction with each step in the methodology described in Section 4.

SECTION 2: RISK DEFINED

A review of applicable FAA and TSA regulations indicates that there is no uniform definition of risk, threat, hazard, or vulnerability in relation to airports and their operations.[1] To support the research objective, it is important to define these terms in order to facilitate assessment of security threats and vulnerabilities, as well as other hazards.

2.1 The Concept of Risk at the National Level

As a starting point for defining terms, it is instructive to briefly understand the broad evolution of security and risk management since the terrorist incidents of September 11, 2001 and the subsequent formation of DHS. Several documents developed by DHS, in coordination with other local, state, tribal, and federal agencies, define terms and form the basis for assessing security vulnerabilities and risk, as well as other hazards, in a strategic and holistic manner:

- **National Infrastructure Protection Plan (NIPP)** – Identifies 16 critical infrastructure sectors and establishes risk-based national plans and programs to address hazards and threats through a private/government sector partnership model. Airports are classified as critical infrastructure under the Transportation Sector. The NIPP defines risk as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.
- **National Preparedness Goal (NPG)** – Establishes the goal to facilitate a secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk. It defines a series of core capabilities and functional targets to address the five mission areas: prevent, protect, mitigate, respond, and recover. The NPG defines risk assessment as a process that collects information and assigns a value to risks to inform priorities, develop or compare courses of action, and inform decision making.
- **National Prevention Framework** – Establishes a process to achieve capabilities to avoid, prevent, or stop a threatened or actual act of terrorism. In the context of national preparedness, the term "prevention" refers to preventing imminent threats. As it relates to risk assessment, the National Prevention Framework indicates that all levels of government, private and nonprofit sector organizations, communities, and households should assess their particular risks to identify capability requirements and mission-essential functions, and to prioritize their preparedness efforts.
- **National Protection Framework** – Establishes a process to achieve capabilities to secure the homeland against acts of terrorism and manmade or natural disasters. As it relates to risk assessment, the National Protection Framework establishes critical tasks, which include the conduct of vulnerability and risk assessments, identification of capability gaps, and coordination of protective measures as a means to mitigate risk.
- **National Mitigation Framework** – Establishes a process to achieve capabilities to reduce loss of life and property by lessening the impact of disasters. The National Mitigation Framework also establishes the need to explicitly assess risk to allow decision makers, responders, and community members to take informed action to reduce their risk and increase resilience.

[1] 14 CFR § 139 – Certification of Airports, 49 CFR § 1540 – Civil Aviation Security: General Rules, and 49 CFR § 1542 – Airport Security

- **National Response Framework** – Establishes a process to achieve capabilities to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. The National Response Framework also establishes the need to address preparedness and response capabilities in relation to identified hazards and threats.
- **National Recovery Framework** – Establishes a process to achieve capabilities to recover efficiently and effectively from an incident. The National Recovery Framework also establishes the need to assess risk, vulnerability, and potential area-wide consequences.

As indicated in these documents, doctrine exists beyond aviation- and airport-specific regulations to support development of a broad-based and consistent methodology to assess security vulnerabilities, threats, and overall risk.

2.2 NIPP Terminology

Because the NIPP addresses sector-specific risk at a national level, the definitions in the NIPP are used below to establish a baseline approach to airport security and risk assessment, consistently with other sectors. These terms are integral elements of risk assessment in airports. They are addressed in more detail in Appendices A and B based on their use in existing risk assessment methodologies.

THREATS AND HAZARDS

In the immediate aftermath of 9/11 and for several years following, national attention focused on security issues. As other incidents of national significance occurred, such as Hurricane Katrina, local, state, and federal agencies began to expand doctrine to include all hazards. While the primary focus of this guidebook is on security issues, it is prudent to consider all risks in creating a resilient airport. Relevant definitions from the NIPP[2] include:

- **Hazard** – Natural or manmade source or cause of harm or difficulty
- **Threat** – A manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property

As commonly used in risk assessments, hazard typically refers to incidents that are not purposeful in nature while threat refers to incidents perpetrated with malicious intent.

CONSEQUENCES

Consequence is defined as the effect of an event, incident, or occurrence including the number of deaths, injuries, and other human health impacts as well as the economic impacts, both direct and indirect, and other negative outcomes to society (NIPP, page 29). For the purposes of assessment, consequence analysis is a component of most risk assessment methodologies, which are summarized in Appendix B, Literature Review.

VULNERABILITY

A vulnerability is a physical feature or operational attribute that renders an organization or physical component open to exploitation or susceptible to a given hazard or threat (NIPP, page 33). Vulnerabilities can be assessed in a number of ways based on the type of hazard or threat being assessed, the type of facility and/or process involved, and the availability of data to support assessment. Government doctrine typically does not provide explicit detail as to how to assess vulnerability. However, sector-based consensus standards exist to identify methods of assessing vulnerability, and are summarized in Appendix B, Literature Review.

[2] National Infrastructure Protection Plan, US Department of Homeland Security, 2013, pages 29–33.

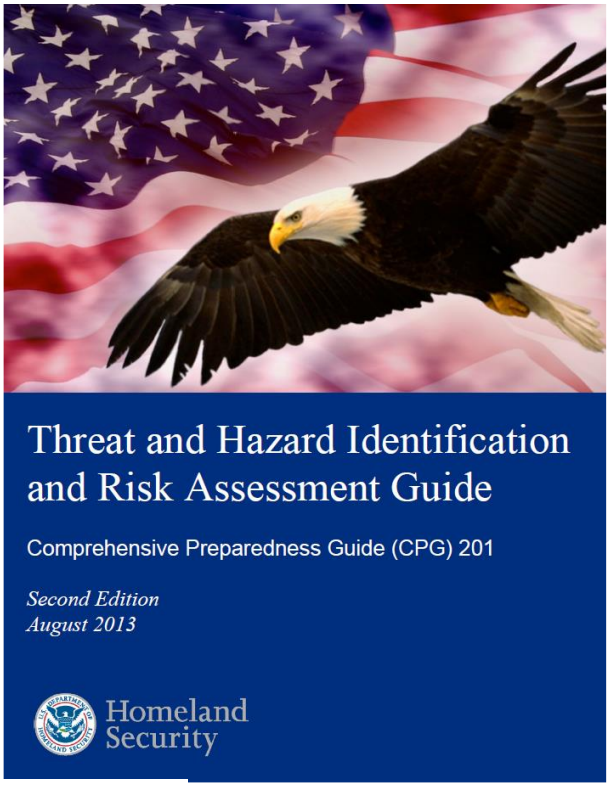
2.3 Threat Likelihood

Threat likelihood is not defined in federal doctrine, but it is an important component of risk, and it is best defined in the American National Standards Institute (ANSI)/American Society of Mechanical Engineers (ASME)-Innovative Technologies Institute, LLC/American Water Works Association (AWWA), J100-10 Standard, Risk Analysis and Management for Critical Asset Protection (J100):

> Threat likelihood is the probability that an undesirable event will occur. With natural hazards, the threat likelihood is the historical frequency of similar events unless there is a belief that the future will differ from the past. With malevolent threats, the likelihood is a function of available intelligence, the objectives and capabilities of the adversary, and the attractiveness, symbolic, or fear-inducing value of the asset as a target.[3]

Methods for assessing threat likelihood are frequently threat- and hazard-specific, and data is often lacking to fully assess likelihood. However, it is an important component of most risk equations and proxy methods can be used when data regarding probability is lacking. Assessment of threat likelihood is discussed in more detail in Appendix B, Literature Review.

Figure 2-1. DHS THIRA Guide



Source: DHS

2.4 Risk Assessment

Identifying a security vulnerability and risk assessment methodology for airports requires discussion of scope and scale. Most government-derived methodologies, such as the DHS Threat and Hazard Identification and Risk Assessment (THIRA) Guide[4], are community-focused and address a broad base of risks across an entire defined population. Other industry-derived consensus standards (discussed in Appendix B) are asset-, facility-, and/or process-focused, and much more tactical in nature.

Research and previous experience using various methodologies indicates the need for a hybrid methodology for airports that focuses primarily at the asset/facility/process level, but gives some consideration to the community approach prescribed in the THIRA Guide. Various industry standards focusing at the asset/facility/process level provide valid models from which an airport-specific risk assessment model can be formed using the general equation below to quantify risk estimations:

Risk = Consequence x Probability x Vulnerability

Quantifying estimations of risk allows ranking of risk and supports decision making regarding risk mitigation.

[3] Risk Analysis and Management for Critical Asset Protection, ANSI/ASME-Innovative Technologies Institute, LLC/AWWA, J100-10, First Edition, July 1, 2010, page 5.
[4] Comprehensive Preparedness Guide 201, Threat and Hazard Identification and Risk Assessment Guide, DHS, Second Edition, August 2013.

SECTION 3: KEY SUCCESS FACTORS FOR SECURITY VULNERABILITY ASSESSMENTS

SVA methodologies from other sectors, stakeholder feedback, and relevant literature were analyzed to identify the following key success factors for planning and conducting SVAs at airports.

3.1 Top-Down Senior Leadership Support and Involvement

Involvement of senior leadership is vital to ensure that SVAs are resourced appropriately, are taken seriously airport-wide, and result in necessary modification of policies, controls, and physical environment to reduce risk. Initial and ongoing senior management participation is recommended to:

1. Assist in scoping the assessment
2. Assist in assigning participants to lead and support the assessment
3. Provide guidance in developing a work plan and timelines
4. Approve resource allocation
5. Support development of mitigation strategies

Senior leadership involvement validates the importance of the process, and signifies the strategic value of risk assessment and mitigation to the overall operation of the airport.

3.2 Designate Points of Emphasis and Requisite Leaders

With senior leadership support, it is important to assign a project manager to oversee the risk assessment and manage the process through its conclusion. Generally, the SVA project manager should be someone with an intimate working knowledge of the airport and an orientation to risk, such as an emergency management, law enforcement, operations, or security representative. It may also be necessary to identify points of emphasis in terms of both function and threat, and to identify and assign personnel who understand various airport functions (functional leads) such as:

- ARFF
- Concessions/properties
- Contracts and administration
- Dispatch/communications/control center(s)
- Emergency management
- Environmental management
- IT
- Law enforcement
- Maintenance (landside, airside, terminal)
- Operations (landside, airside, terminal)
- Safety and/or risk
- Security and badging

Drawing on knowledge and expertise from a wide range of sources is essential to ensure that important risk factors are considered. Various airport operational personnel, serving as functional leads for the SVA, generally have the most complete understanding of the criticality and sensitivity of individual functions, systems, and interdependencies that support their assigned operations. Thus, they are in the best position to identify consequences of threats in their operational environments.

Functional leads can facilitate assessment planning, assist in determining potential consequences for specific threats, and support development of mitigation strategies. In addition, functional leads may serve as coordinators for various external stakeholders (i.e., those outside of direct airport management control) such as:

- Air cargo operators
- Airline station managers
- Baggage handling companies
- Contract security services, if applicable
- Fuel providers
- Ground transportation providers (parking, rental car, and bus/livery/taxi services)
- Skycap and janitorial service companies
- Terminal concessionaires
- Vendors

If the assessment is to focus on risk-based mitigation measures and response resources internally and in concert with federal partners, it is advisable to assign one or more functional leads to coordinate with government partners including Customs and Border Protection, FAA, FBI, TSA, and others as warranted. Functional leads can serve as a trusted agent and single point of contact for various government stakeholders throughout the risk assessment process.

3.3 Define the Process

The SVA project manager should define and document the process for conducting the SVA, and use tools to facilitate and standardize the process. While this guidebook provides a methodology and tools, defining additional processes to manage team members ensures consistency, avoids duplication of effort, and allows for conflict resolution during the assessment.

Defined managerial processes coupled with the SVA methodology provide an overall construct for disparate functional leads and stakeholders to conduct the SVA. Process definitions should include:

- Who is the project manager responsible?
- Who are the functional leads and what are their points of emphasis?
- What are the specific steps to be followed?
- How are differences of opinion and/or discrepancies in data to be resolved?
- What approvals are necessary at each step in the process?
- What are the documentation requirements?
- What are the reporting requirements throughout the process?

The process outlines how functional leads elevate proposed changes in SVA methodology to the project manager for approval. Approved modifications to SVA processes should be shared among all participants to promote use of best practices.

The project manager should serve as the collection point for data and documentation throughout the process, and should work with senior leadership to identify interim (if applicable) and final reporting requirements.

3.4 Involve Technical Experts

Technical personnel, such as security and IT specialists, and those with experience in using best practices, can provide an understanding of existing physical security and security technology, including vulnerabilities and potential benefits, costs, and performance impacts associated with mitigation measures. For specific critical functions and concerns (e.g., airfield lighting, cybersecurity, structural integrity, etc.), technical experts may be necessary to fully assess risks and mitigation choices. Technical expertise may be available internally or may require external support via contractors or other stakeholders.

3.5 Segment the SVA

Generally, SVAs provide the most use when they are comprehensive in consideration of threats, and assets or functions. However, if the scope and scale are daunting and/or the resources available to support the SVA are lacking, it may be beneficial to conduct a series of narrower SVAs focusing on specific assets or functions within the airport. Recommendations for segmenting SVAs include:

- Identify critical threats of concern, prescreen assets, and choose an asset(s) to assess that have the highest perceived consequence and/or vulnerability to threats of concern
- Develop a prioritized list of other assets and a timeline to perform SVAs in order of priority
- Consider assessing single points of failure (i.e., those assets or functions that have no backups or workarounds) first.

Segmenting SVAs assists in making them more manageable, reduces the size of each assessment, and reduces scheduling burdens. In addition, segmenting airport operations provides a means of initial ranking of assets and functions to determine the order in which SVAs are performed and which units may require more frequent assessment. A common potential segmentation opportunity exists in performing a cyber-SVA as a separate function to an operational SVA. While cyber functions are inextricably linked to airport operations, generally the focus areas and procedures to assess the security of cyber assets are quite different and involve different subject matter expertise relative to other functional assets.

3.6 Document Results

SVAs should be documented, maintained, and tracked to ensure that assigned personnel are held accountable for implementing procedural, physical, and technological risk-mitigation measures identified during the process. Documentation also informs capital budgeting and planning, and provides an opportunity to audit various operations to ensure compliance with airport security regulations, policies, and procedures.

Documentation may take the form of simple documents or databases cataloging SVA results, mitigation recommendations, assignees, recommended due date or timeline, and status of each recommendation. Documentation templates are provided in Appendix C, Airport Security Vulnerability Assessment Checklists, and Appendix G, Airport Security Vulnerability Assessment Report Template.

3.7 Provide SVA Tools and References

Those charged with conducting SVAs within airports require tools such as checklists and standard formats to help ensure a consistent and standardized approach throughout the airport. Tools to facilitate conducting an airport SVA are provided in Appendix C to support:

- Ease of understanding and use
- Automation using common software
- Assessment of threat probability, asset vulnerability, and consequences

While efforts have been made to provide tools for all sizes of airports, variances in conditions may require refinement to support airport-specific needs. In addition to tools provided in Appendix C, information regarding airport assets—including specifications, cost and maintenance data, and interdependencies—is useful to identify critical assets, single points of failure, and repair/replacement costs.

3.8 Document Benefits

Managing any kind of business or organization is, at its core, about managing associated risks. Managing risk is particularly important in airport operations, which:

- Entail multiple simultaneous and inherently hazardous operations
- Encompass hundreds or thousands of people
- Require costly resources with potentially costly consequences when subjected to certain threats

Thus, SVAs support airport operations and business functions by ensuring that the greatest risks are identified and addressed on a continuing basis. Additionally, SVAs:

- Enable the people most closely associated with specific airport functions to use their expertise to develop mitigation measures to protect those functions
- Serve as a valuable first step in developing Security Master Plans
- Provide an opportunity to alert airport personnel of external risks, to avoid risky practices, and to identify suspicious activity (with improved risk communication, personnel across the airport become a force multiplier in preventing security threats from occurring)
- Provide an open forum for airport management to reach consensus on the greatest risks and how to mitigate them
- Provide efficient means of communicating risk and mitigation strategies to senior leadership
- Provide information necessary to perform strategic budgeting (see Section 6 for more details)

SECTION 4: RECOMMENDED AIRPORT SVA METHODOLOGY

The recommended SVA methodology for airports, provided below, is based on reviews of methodologies used in other sectors, assessments of stakeholder feedback, and identification of key success factors. The methodology borrows from existing processes and adapts them to facilitate identification of:

1. Relevant airport assets and functions of concern
2. Relevant reference threats for airports
3. Quantitative and qualitative risk identification and rating processes that are valid, flexible, and easy to implement

Sections 4.5 and 4.6 describe steps to identify threat likelihood and vulnerability that aim to streamline both the risk identification process and the prioritization of assets and hazards. Aside from the airport focus and recommendations regarding threat likelihood and vulnerability, the suggested methodology is similar to those used in other critical infrastructure sectors and relies on the equation:

Risk = Consequence x Probability x Vulnerability

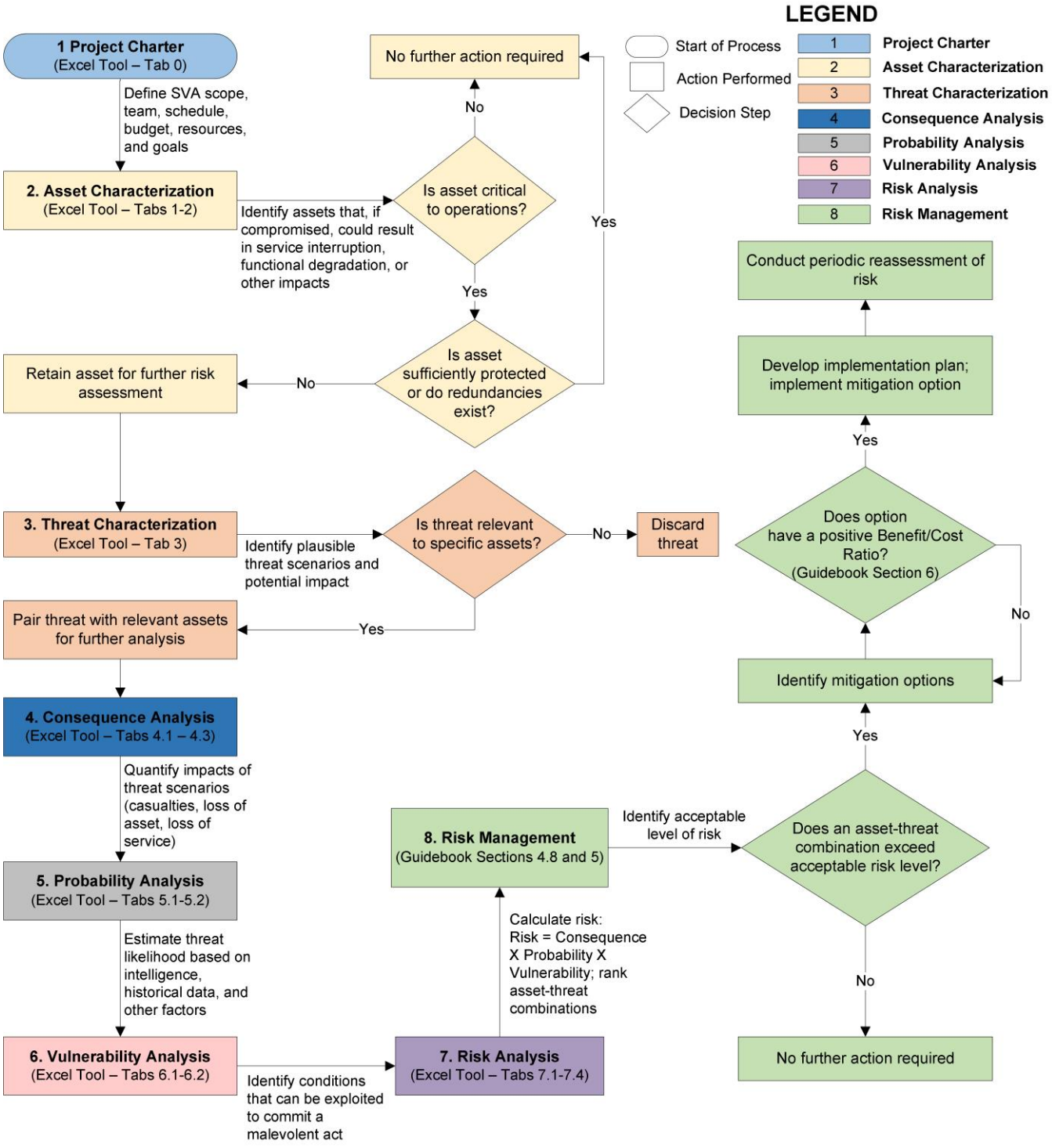
The eight steps recommended herein are summarized in Figure 4-1, and are consistent with methodologies identified in the Literature Review (see Appendix B).

Figure 4-1. Airport SVA Steps

To support benefit/cost analysis, it is desirable to express risk in economic terms. For this reason, consequence analysis is expressed in dollars, while probability and vulnerability are expressed in percentages. When applied in the risk equation, the resulting risk for quantitative assessment is based in monetary terms. Qualitative assessment may result in risk categories.

Steps and processes recommended for an airport SVA methodology are described below and are presented in the context of the SVA Process Flow Diagram in Figure 4-2.

Figure 4-2. Airport SVA Process Flow Diagram



4.1 Step 1: Project Charter

At the outset of the process, the authorizing airport authority should develop a project charter that identifies the purpose, scope, and scale of the desired SVA, as well as the resources assigned and available to conduct it. The charter should identify the following:

A. Scope – The scope should identify assets and threats of concern and the overall goal of the SVA as described below:
1. Comprehensive versus limited with respect to operations (e.g., airside, landside, terminal, cyber)
2. Quantitative versus qualitative with respect to risk and risk parameters
3. Comprehensive versus limited with respect to threat (e.g., insider threats, cyber threats, armed attack threats, etc.)
4. Desired goal upon completion of the SVA (e.g., identify risk and mitigation measures relative to perimeter breaches *or* identify prominent insider threats *or* perform comprehensive SVA to set priorities for capital budgeting and operational modifications)

B. Assigned Team – The assigned team to conduct the SVA should include a leader, team members, and stakeholders:
1. Project Manager – Identify a project manager who has knowledge of the SVA methodology and authority to lead the process
2. Team Members – Add appropriate functional leads to the team based on the assets/functions included in the scope
3. Stakeholders – Identify relevant external stakeholder representatives, including their contact information, based on the assets/functions included in the scope

C. Schedule – State the desired completion date and milestones in order to communicate expectations, schedule tasks, and define resources

D. Budget/Resources – Identify the budget, available resources, and accounting requirements to provide the project manager with appropriate information to manage the process

E. Additional Instructions – Include any additional instructions regarding the scope, purpose, regulatory concerns, or other factors that will assist in completing the SVA effectively and efficiently

The project charter provides the SVA Project Manager and team members with the direction and requirements necessary to begin. A project charter format is provided in Appendix C, Table C-1, and in the SVA Tools (Tab 0 – Project Charter).

4.2 Step 2: Asset Characterization

The purpose of asset characterization is to determine the assets that, if compromised by a threat, could result in interruption of service, functional degradation, injuries, fatalities, detrimental economic impact, or any combination thereof. The result is a prioritized list of critical assets to be evaluated in additional steps. To facilitate asset characterization, the following information should be identified pursuant to the defined SVA scope:

1. What facilities/functions are critical to airport operations (or to operations in the SVA scope)?
2. Within critical facilities and/or functions, what individual assets are critical, and are they dependent on one another or individually critical?
3. Which assets are most likely to cause injury, death, or major losses if rendered inoperable?
4. Do interdependencies exist for critical assets such as power, fuel, water, and lifelines (police, fire, and medical)?

5. What mitigation measures or redundancies exist to protect the asset or the function it serves?
6. Which assets are most important based on possible consequences?

Table 4-1 lists typical airport assets to consider. Pursuant to the identified scope, the team may choose to add more tactical or granular assets (e.g., emergency generators) or group assets based on area.

Table 4-1. Airport Reference Assets

Category/Asset
A. Airside Operations and Secured Areas
1. Access Control System
2. Aircraft Hydrant Fueling System
3. Aircraft Rescue & Firefighting Facilities/Resources
4. Airfield Navigation Systems
5. Airport Authority Operations & Maintenance Facilities
6. Cargo Facilities
7. Catering Facilities
8. Checked Baggage Screening/Operations/Makeup Areas
9. Concession Storage Areas
10. Deicing Systems
11. Federal Inspection Stations
12. Fuel Farm
13. General/Business Aviation Areas
14. Ground Run-up Enclosure
15. Jet-bridge Access
16. Movement Areas (runways and taxiways)
17. Non-movement Area Vehicle Access Points
18. Perimeter Fencing
19. Perimeter Intrusion Detection System
20. Vehicle Gates
B. Terminal Operations (Public)
1. Baggage Claim
2. Concessions
3. Security Screening Checkpoints
4. Ticket Counters/Automated Check-In Areas

Category/Asset
C. Landside Operations
1. General Traffic/Curbside Management Operations
2. Ground Transportation Operations
3. Parking Operations
4. Rental Car Operations
D. Infrastructure
1. Airport Authority Administrative Offices
2. Airport Authority Ground Vehicle Fueling Systems
3. Audio Communication Systems
4. Cellular Communication Systems
5. Common Use Information Technology/Networks
6. Dispatch/Communications Centers
7. Electrical Power Services
8. First Responder Communication Systems
9. Heating, Ventilation, Air Conditioning (HVAC) Systems
10. Law Enforcement Facilities and Resources
11. Mechanical, Electrical, Plumbing (MEP)
12. Natural Gas Services
13. Potable Water Services
14. Radio Communications Systems
15. Sewer Systems
16. Stormwater Systems
17. Vendor Deliveries
18. Vertical Circulation Systems
19. Video Communication Systems
20. Video Surveillance Systems
21. Waste Management Systems

To facilitate asset identification, an Airport Critical Asset Identification Checklist based on this table is provided in Appendix C, Table C-2.

Each asset deemed critical should be fully characterized using the Asset Characterization Checklist provided in Appendix C, Table C-3 (also see Tab 2 – Asset Characterization in the SVA Tools). The Asset Characterization Checklist focuses on the following characteristics:

1. Asset function – What is the primary function of the asset?
2. Asset criticality – If the asset is out of service, what are the potential ramifications (degradation of service, partial/full airport closure, injuries/fatalities to patrons and/or employees, economic impacts)?
3. Down-stream dependencies – What assets/functions are reliant on the asset?
4. Up-stream dependencies – What assets/functions does the asset rely on to function properly?
5. Existing mitigation measures or security hardening – What measures are in place to protect the asset from specific threats?
6. Existing backups – Are redundant systems available that are sufficient to take the place of the asset? For what period of time? What is required to operate backups?
7. Workarounds – What measures can be implemented temporarily to operate without the asset and are those measures cost effective?
8. Replacement cost – If the asset is destroyed, what is the current cost of a replacement asset and amount of time required to perform asset replacement?

Identifying these characteristics enables asset prioritization based on criticality and provides information necessary to perform additional SVA steps, including consequence analysis, identification of potential mitigation strategies, and benefit/cost analysis. If existing mitigation measures, security hardening, and/or redundant systems are available to protect the asset or function, the team may choose to eliminate the asset from additional assessment.

4.3 Step 3: Threat Characterization

Threats must be identified and characterized to determine their validity for the airport, both in general and in relation to specific critical assets. Threat characterization seeks to identify relevant asset-threat combinations to assess in the remainder of the SVA process (i.e., those asset-threat combinations with a medium or high estimation of potential impact). Upon conclusion of this step:

1. A list of malevolent threats will be identified (threats that have a reasonable likelihood of occurrence will be addressed in consequence analysis)
2. Threats will be addressed relative to identified critical assets and their relevance will be ranked based on a broad estimation of potential impact (high, medium, or low)
3. Critical assets linked to specific threats will be identified to facilitate cross-asset comparison of risk

In addition to reference threats, characteristics of the perpetrator of a malevolent threat should be considered. The most common factor to consider in threat characterization is the perpetrators' status as insiders or outsiders. This is particularly true for airports given the importance of maintaining control within Secured and Sterile Areas. An insider threat involves one or more perpetrators with access and inside knowledge of the airport layout, critical assets and systems, security measures, and vulnerabilities that could be exploited relative to a specific malevolent threat. Conversely, an outsider is someone who has not worked at the airport in any capacity. Generally, insider threats present more risk, as insider

knowledge may enable the perpetrator to overcome existing security measures, and increases the probability of the threat occurring.

The Threat Characterization Tools provided in Appendix C3 attempt to distinguish between asset-threat combinations that are applicable to outsiders versus insiders. Insider and outsider threats are analyzed in more depth in Section 4.6, Vulnerability Analysis. Appendix C3 also provides a list of airport-specific reference threats and their definitions.

The Asset-Threat Characterization Tool is intended to provide a systematic process to identify the most plausible asset-threat combinations based on estimated impact. Determination of threat applicability for specific assets may require a committee approach to ensure a well-informed process. Committees to determine asset-threat relevancy may include operational SMEs, engineers, security, law enforcement, ARFF, or other specialties.

A blank version of the tool is provided in Appendix C3, Table C-5. To simplify threat characterization, a completed version is provided in Tab 3 of the SVA Tools. If used, the SVA project team should review the content to ensure consensus with the conclusions and/or to identify any additional asset-threat combinations that should be assessed. A list of reference asset-threat combinations derived from the completed version is provided in Table C-6 and lists each airport asset with relevant threats. This list can be used to perform consequence, probability, and vulnerability analysis, or it can be customized to fit local needs. Alternatively, the SVA project team may choose to evaluate all asset-threat combinations independently.

In some cases, a threat may have no impact on an asset due to the inherent design of the asset. In other cases, security hardening, redundancy, or other mitigation measures may render a threat less probable. The SVA project team can choose to rank threats relative to each critical asset, and the ranking can then be used to select asset-threat combinations to evaluate in remaining steps.

CYBERSECURITY

IT and networks are addressed as assets that can be assessed in relation to relevant threats listed above. However, IT-specific threats, such as hacking and other cyber intrusion, generally require a specialized team to assess risks. Absent a team of internal IT professionals, a full assessment of cyber risks may require external support, particularly for activities such as penetration testing, which assesses the ease at which a network or system can be penetrated (hacked). Considerations for performing a cybersecurity risk assessment are provided in Appendix D.

NATURAL HAZARDS

Many other methodologies identified during the literature review use an all-hazards approach to risk assessment, most notably the J100 standard and the DHS THIRA process. With minor procedural modifications, SVA processes provided herein can be applied to natural hazards. In many cases, data regarding probability of natural hazards is readily available through government and academic sources. Considerations for performing a natural hazard risk assessment are provided in Appendix E.

4.4 Step 4: Consequence Analysis

With a full understanding of plausible asset-threat combinations, analysis of consequences can be performed to estimate potential losses from the exposure of threats to specific assets. Assessment of various sector-based standards and FEMA guidelines regarding benefit/cost analysis and accounting for consequences yields five primary components that are applicable to airports as identified in Table 4-2.

Table 4-2. Components of Consequence Analysis for Airport SVAs

Component	Description
Number of Fatalities	Estimate of the number of fatalities anticipated for a specific asset-threat combination
Number of Injuries	Estimate of the number of injuries anticipated for a specific asset-threat combination
Displacement/Workaround Costs	Estimate of the cost of temporary displacement and/or workaround costs necessary to sustain operations
Replacement/Repair Costs	Estimate of the cost of repair or replacement cost for assets damaged due to a specific threat
Loss of Service Costs	Estimate of the loss of service costs associated with any downtime or reduced service potential due to a specific threat

4.4.1 Quantitative Approach

Using quantitative analysis, the first step in approximating consequence is to determine per unit rates for the five components of loss, as indicated in Table 4-3. All estimates provided are based on established government and industry standards for estimating losses. Estimates and methodology to calculate losses are also consistent with other risk assessment methodologies described in the literature review.

Table 4-3. Per Unit Loss Estimates for Consequence Analysis

Component	Estimate	Source and Description
Loss Estimate per Fatality	—	To be determined in consultation with airport management, local emergency management, or other source.
Loss Estimate per Injury	—	To be determined in consultation with airport management, local emergency management, or other source.
Displacement/ Workaround Cost	$1.76/ft^2/ month	Supplement to the Benefit/Cost Analysis Reference Guide, FEMA, June 2011. Table 11: HAZUS MR3 Displacement Costs (2008), Government Facilities. 2008 figure ($1.46) adjusted to 2019 dollars using Consumer Price Index (CPI) Inflation Calculator.[5]
Replacement/ Repair Cost	$400/ft^2	Based on average of per square foot cost of $200 for various types of buildings indicated in the Online Construction Estimating page of BuildingJournal.com[6] + 100% content value as indicated in Supplement to the Benefit/Cost Analysis Reference Guide, FEMA, June 2011. Table 10: HAZUS MR2 Default Contents Value Based on Percentage of Structure Value, Government Facilities.
Loss of Service Cost to Airport	$211/ passenger	Based on 2005 data: 737,186,789 total passengers in the United States per FAA statistics[7] and the total per day estimate of cost of having no air transport in the US of $320 million[8] which yields a 2005 figure of $158/passengers. Estimate is adjusted to 2019 dollars using CPI Inflation Calculator.

[5] **CPI Inflation Calculator:** https://www.bls.gov/data/inflation_calculator_inside.htm
[6] http://www.buildingjournal.com/construction-estimating.html
[7] https://www.faa.gov/airports/planning_capacity/passenger_allcargo_stats/passenger/previous_years/#2005
[8] Economic Effects and Costs of a Temporary Shutdown of an Airport – Review and Case Study, Katrien, De Langhe, et al, Department of Transport and Regional Economics, University of Antwerp, July 15, 2013.

FATALITY AND INJURY ESTIMATES

In addition to the per unit data provided in Table 4-3, fatality and injury estimates require factors based on threat type and airport size. Proxy rates for injury and fatality, provided in the SVA Tools Tab 4.1 Table 4-4, can be used in concert with passenger throughput data to calculate rough order of magnitude (ROM) fatality and injury estimates for specific threats. Consensus should be sought among SVA team members regarding the rates provided in the SVA Tools. Alternative rates or calculations may be achieved with support from outside resources such as emergency management or local/regional homeland security officials.

DISPLACEMENT/WORKAROUND, REPAIR/REPLACEMENT, AND LOSS OF SERVICE COSTS

Given estimated rates for displacement/workaround costs, replacement/repair costs, and loss of service costs, additional data sets can be used to calculate estimates for each parameter. The three parameters are described below along with their estimated rates:

1. Displacement/workaround costs – Also requires an estimate of area impacted and duration of downtime; ($1.76/square foot/month)
2. Replacement/repair costs – Also requires an estimate of area impacted; ($400 per square foot)
3. Loss of service – Requires an estimate of duration of downtime, percentage of airport impacted, and passenger throughput; ($211/passenger)

The SVA Tools Tab 4.1 provides example data sets for the estimated area impacted and time of displacement/workaround, based on experiential data for each threat. These estimates can be used in conjunction with the rates above to calculate displacement/workaround, replacement/repair, and loss of service costs. Factors should be analyzed and agreed to by the SVA team and are highly likely to be differ based on airport size.

LOSS DUE TO THEFT

While not one of the five primary components of consequence shown in table 4-2, it may be appropriate based on the SVA scope to consider loss due to theft. Estimates of loss due to theft can be developed based on passenger throughput, rates of theft per 100,000 enplanements, and the average loss per theft. There is currently no data available regarding theft rates at airports, but a research document developed at Rutgers, the State University of New Jersey suggests a rate among airport employees of between 3.39 and 5.00 thefts per thousand enplanements.[9] For the purposes of estimating worst-case loss potential, an average theft rate of 4.195 per 1000 is used in the example calculations provided in Table 4-4. As with other proxy measures, it is advisable to substitute known local theft rates if they exist.

Table 4-4. Example Estimates: Worst-Case Loss Potential Due to Theft

Airport Size	Average Cost per Theft[10]	Average Theft Rate	Passengers/ Day	Potential Loss/Day
Small Hub	$559	0.004195	5,886	$13,802
Medium Hub	$559	0.004195	26,449	$62,024
Large Hub	$559	0.004195	124,786	$292,624

[9] Solans, Nerea Marteache, "Employee Theft from Passengers at U.S. Airports: An Environmental Criminology Perspective," Rutgers, the State University of of New Jersey, 2012, https://rucore.libraries.rutgers.edu/rutgers-lib/39449/PDF/1/play/

[10] 2018 National Retail Security Survey, National Retail Federation, Page 12, https://cdn.nrf.com/sites/default/files/2018-10/NRF-NRSS-Industry-Research-Survey-2018.pdf.

TOTAL ESTIMATED COSTS BY THREAT

Using the factors described throughout this section or alternatives derived locally, total estimated consequences for specific threats can be developed using the totals for each of the components indicated in Table 4-2, with the addition of loss due to theft (if applicable). This total provides an estimate of the total consequence of a threat applied to a specific asset.

Refer to Appendix C4, Consequence Analysis Tool for more information.

4.4.2 Qualitative Approach

In lieu of determining monetary consequences, the SVA project team may choose to use consensus-based qualitative consequence rating categories for each asset-threat combination, such as:

- Little to No Impact
- Low Impact
- Moderate Impact
- High Impact
- Catastrophic Impact

Using qualitative measures, generally those asset-threat combinations that fall below the Moderate Impact category would be eliminated from consideration for the balance of the SVA. While this method simplifies the process, it may yield less accurate measures of risk for each asset-threat combination, which will also impact the benefit/cost analysis.

4.5 Step 5: Probability Analysis

Probability analysis is the estimate of the likelihood of each specific threat occurring, and is generally based on intelligence or historical data, estimates of the asset's attractiveness to the perpetrator, and the ease with which the threat can occur. Probability is a measure of the likelihood, degree of belief, frequency, or chance that a particular event will occur in a defined period (usually one year). For malevolent threats, the relative attractiveness of the specific target is based on evaluation of alternative targets and likelihood of success.

Generally, larger airports have a higher degree of probability for certain risks than medium and small airports. To thieves, larger airports represent a bigger payout, and to terrorists, larger airports represent a more valuable target.

Also, specific threats may have differing probabilities based on location within an airport. For example, the probability of an active shooter incident in public areas is much greater than that of a similar incident in Sterile or Secured Areas of an airport. Insider versus outsider considerations relative to location are also important factors to consider in assessing probability.

In general, the probability of attacks involving firearms, explosives, or infectious agents are very low within all types of airports. However, probabilities vary to some degree based on airport size, location, and insider/outsider considerations. The status of a perpetrator as an insider tends to increase the probability of armed attack, assault, sabotage, and theft, specifically when access to Sterile and Secured Areas is required, and when knowledge of airport assets and layout improve the odds of perpetrating a threat. It is important to engage law enforcement, security experts, and other SMEs to review and revise probability estimates to ensure consistency in how estimates of probability are derived. Generally, rare and low probability items are eliminated from further assessment. However, consideration should be

given to those threats with very high consequences; consensus on whether or not to eliminate these threats should be sought within the SVA team.

4.5.1 Quantitative Approach

An example probability scale that can be used for quantitative analysis is provided in Table 4-6.

See Tabs 5.1 – Probability Outsider and 5.2 – Probability Insider in the SVA Tools for examples of ROM probability estimates, which were arrived at based on the research team's experiential data. These numbers can be changed in the Tools if more accurate estimates are available for the specific airport being assessed. Any threat-based probabilities should be arrived at through consensus among the SVA team members.

Table 4-5. Example Probability Scale

Rating Category	Rating
Not Probable/Rare	0.10
Low Probability	0.30
Probable	0.50
Highly Probable	0.70
Near Certain Probability	0.90

4.5.2 Qualitative Approach

In lieu of assigning numerical values for probability, the SVA project team may choose to use consensus-based qualitative probability rating categories for each asset-threat combination, such as:

- Not Probable/Rare
- Low Probability
- Probable
- Highly Probable
- Near Certain Probability

Using qualitative measures, generally those asset-threat combinations that fall in the Not Probable/Rare and Low Probability categories would be eliminated from consideration for the balance of the SVA. While this method simplifies the process, it may yield less accurate measures of risk for each asset-threat combination, which will also impact the benefit/cost analysis.

4.6 Step 6: Vulnerability Analysis

The third and final component of the risk equation is vulnerability, which serves as a measure of the organizational, physical, and technical conditions that can be exploited by a perpetrator to improve the probability of success of committing a malevolent act. In contrast to probability (described in Section 4.5), which focuses on the likelihood of occurrence of a specific threat type, vulnerability focuses on the asset's susceptibility to a threat. Conditions that determine the level of vulnerability of a given asset to a specific threat may include:

- Asset characteristics – Building/construction standards, level of physical security, and equipment characteristics
- Technology – Systems available to deter, detect, and defend against threats
- Operational Practices – Plans, policies, procedures, training, quality assurance, and personnel practices

Tasks to support vulnerability analysis include:

1. Review and document pertinent assets, equipment, technology specifications, and facility layout
2. Identify countermeasures, mitigation measures, and other impediments to threats that provide deterrence, detection, or delay capabilities
3. Assess local supporting operational response measures
4. Identify processes within the airport that impact threat potential

Estimates of conditional probabilities indicate success and failure rates for a particular malevolent threat occurring based on location and type of threat. The airport reference assets (Table 4-1) are located in one of three areas: Public, Sterile, or Secured. In general, public areas are much more vulnerable to malevolent threats than Sterile and Secured Areas.

While significant variation exists among airports as to systems, technology, and operational practices, regulations that define standards for airport operations and security (14 CFR § 139, Certification of Airports and 49 CFR § 1542, Airport Security) allow general assessment of airports and development of proxy measures for vulnerability.

4.6.1 Quantitative Approach

Tabs 6.1 – Vulnerability-Outsider and 6.2 – Vulnerability-Insider in the SVA Tools provide example measures, which are used in the risk calculations. These measures are derived from the research team's experiential data and event tree analyses. In the SVA Tools, modifications to Tabs 6.1 and 6.2 regarding vulnerability will automatically feed the risk calculation formulas in Tabs 7.1 and 7.2.

SVA project teams should perform local event tree analysis or another form of vulnerability analysis to validate estimates of vulnerability. An example event tree is provided in Appendix C5, Figure C-1. When developing asset-based vulnerability estimates, the SVA team should engage law enforcement, airport security experts, and other SMEs to review and revise proxy measures if there is reason to believe that conditions at a specific airport may vary.

In summary, general principles used to develop proxy measures include:

1. Security measures in place to maintain Sterile and Secured Areas within airports significantly reduce the vulnerability of those areas to malevolent threats.
2. The level of vulnerability within Sterile and Secured Areas at airports is significantly higher for insider threats as opposed to outsider threats. Most insider threats are associated with personnel gain (theft).
3. By their nature, publicly accessible areas within airports are more vulnerable to a broader spectrum of malevolent threats, and may hold value in making a political statement.

4.6.2 Qualitative Approach

In lieu of assigning numerical values for vulnerability, the SVA project team may choose to use consensus-based qualitative vulnerability rating categories for each asset-threat combination, such as:

- Not Vulnerable (e.g., Secured Areas; near zero outsider vulnerability and low insider vulnerability; areas where substantial mitigation measures have been employed)
- Moderately Vulnerable (e.g., Sterile Areas; residual risk from screening errors; increased insider vulnerability; modest mitigation measures)
- Highly Vulnerable (e.g., public areas with few mitigation measures beyond human intervention)

Using qualitative measures, generally those asset-threat combinations that fall in the Not Vulnerable category are eliminated from consideration for the balance of the SVA. While this method simplifies the process, it may yield less accurate measures of risk for each asset-threat combination, which also impacts the ability to accurately perform benefit/cost analysis.

4.7 Step 7: Risk Calculation and Risk Ranking Methodology

Risk ranking allows management to focus resources on those asset-threat combinations that pose the greatest risk to airport operations and are outside of acceptable limits of risk.

4.7.1 Quantitative Approach

The recommended quantitative methodology provided in this guidebook is based on the desire to use benefit/cost analysis to support decisions regarding risk mitigation. Thus, the consequence factors yield monetary results for risk when combined with unitless estimates of probability and vulnerability. The SVA Tools calculate risk automatically based on input of the consequence, probability, and vulnerability variables in rank order based on asset-threat combinations.

Quantitative risk analysis measures are essentially consequence measures discounted by probability and vulnerability. The desire is to address those asset-threat combinations with highest aggregate consequence, probability, and vulnerability. Experience in conducting SVAs indicates that explosive attacks generally rise to the top due, in large part, to the extraordinarily high consequences of such incidents. In general, threats typically fall in the categories indicated in Table 4-7, particularly for publicly accessible assets and threats perpetrated by insiders.

Table 4-6. Experiential Data – Threat Type and Risk Rankings

	Threat	Risk Value
1	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED	High
2	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED	
3	Attack: Explosives <=15kg TNT Equivalent	
4	Arson	Medium
5	Vehicle as a Weapon	
6	Armed Attack	
7	Attack: Release of Infectious Agents	
8	Attack: Explosives <=5kg TNT Equivalent	
9	Sabotage	Low
10	Civil Disorder	
11	Vandalism	
12	Assault	
13	Trespassing	
14	Theft	

Risk derived using the methodology suggested in this document provides airport management with prioritized asset-threat combinations. In using risk rankings, it may be necessary to define a level of acceptable risk and then mitigate the asset-threat combinations at and above that level. For example, if

airport management chooses $5,000,000 as the limit of acceptable risk, based on insurance or limits of liability, the number of asset-threat combinations for which mitigation is necessary may be reduced based on the estimated risks that fall below that value.

4.7.2 Qualitative Approach

If the SVA team chooses to use qualitative rating categories for probability and impact, asset-threat combinations can be evaluated based on a two-factor approach using a matrix or heat map presented in Table 4-8.

Table 4-7. Heat Map for Qualitative Consideration of Probability and Impact

		Impact →				
	Probability	**Little to No Impact**	**Low Impact**	**Moderate Impact**	**High Impact**	**Catastrophic Impact**
↑	**Near Certain**	No action necessary	Consider mitigation	Consider mitigation	Mitigation recommended	Mitigation recommended
	High	No action necessary	Consider mitigation	Consider mitigation	Mitigation recommended	Mitigation recommended
	Moderate	No action necessary	No action necessary	Consider mitigation	Consider mitigation	Mitigation recommended
	Low	No action necessary	No action necessary	Consider mitigation	Consider mitigation	Mitigation recommended
	Near Zero	No action necessary	No action necessary	No action necessary	Consider mitigation	Consider mitigation

If qualitative probability and impact categories are used, those asset-threat combinations that fall in yellow and red categories should be ranked to yield a prioritized list of asset-threat combinations for which mitigation should be considered. Benefit/cost analysis can be performed using costs of impact for each asset-threat combination (in lieu of risk).

4.8 Step 8: Risk Management

Risk Management is the process of reviewing prioritized risks and identifying methods to mitigate them. Through consultation with the SVA team and with concurrence of senior leadership, Step 8 defines acceptable levels of risk and countermeasures, consequence mitigation, and resilience options specific to asset-threat combinations of concern. As indicated in many of the other methodologies reviewed (see Appendix B, Literature Review), actions under this step may include:

- Determine if risk levels for critical assets are acceptable
- Identify potential physical modifications or infrastructure improvements to mitigate risks
- Identify backups and redundancies to improve resiliency
- Identify procedural/operational modifications to mitigate risks
- Establish cost estimates for mitigation strategies, operational countermeasures, and redundancies
- Evaluate alternatives based on feasibility and benefit/cost analysis
- Identify specifications and sources for chosen mitigation strategies, operational countermeasures, and redundancies

These actions should answer these important questions:

- What benefit does each mitigation option convey and how are benefits valued?
- What is the cost of each mitigation option?
- How is each mitigation option managed over time?
- What is the lifecycle of each mitigation option?
- When is it prudent to update risk analysis?

This step supports decisions to select specific countermeasures and consequence reduction options based on acceptable levels of risk and cost. Ultimately, senior leadership must determine acceptable risk levels and balance risk with the costs of mitigation. Ongoing risk management functions include:

- Identifying, measuring, and controlling risks at an acceptable level
- Monitoring and evaluating the effectiveness of implementation
- Operating selected options with corrected actions, as needed
- Conducting periodic repetition of the full risk management cycle

Additional information regarding risk management is provided below.

4.8.1 Roles and Assignments

In addition to the SVA team, specific SMEs may be needed to help identify and evaluate mitigation strategies. Examples include:

- **Structural Engineers** – Architectural, electrical, mechanical and other specialized engineering disciplines can assist in identifying physical mitigation strategies
- **Information and Systems Technologists** – Cybersecurity and systems specialists can assist in identifying systems-based hardware and software solutions, as well as integration needs
- **Emergency/Security Planners** – Planning specialists can assist in identifying plans, procedures, training, and exercise programs to mitigate certain risks and to facilitate an effective security posture among personnel
- **Cost Estimators** – As part of the functions described above or as a separate function, cost estimators can support financial estimations to allow benefit/cost analysis and ranking of mitigation options

As mitigation options are identified, these SMEs, in collaboration with the SVA team, can fully develop capital and operational cost information, define resource needs, and identify implementation strategies.

4.8.2 Developing Countermeasures and Mitigation Options

In general, mitigation measures fall into three primary categories:

1. **Physical Security** – Design and structural features such as bollards, fences, and other barriers, blast-resistant construction, etc.
2. **Security Technology** – Systems and technology such as Access Control Systems, Perimeter Intrusion Detection Systems, video surveillance, situational awareness tools, etc.
3. **Processes and Procedures** – Personnel-focused strategies such as emergency and security plans and procedures, personnel qualifications, training and exercises, etc.

For each of these categories, governmental and consensus-based guidelines and standards exist that provide implementation and performance criteria to effectively mitigate specific types of risk. For example, physical security and security technology standards include those developed by ANSI, ASME,

ASTM International, Building Industry Consulting Service International, and many others. Process and procedural standards include those promulgated by federal agencies, such as the FEMA Comprehensive Preparedness Guides, National Incident Management System (NIMS), and the Homeland Security Exercise and Evaluation Program (HSEEP), among others, as well as guidelines developed by ASIS International and other industry trade organizations. Such standards and guidelines should inform and support choosing, planning, and implementing mitigation options.

Steps to develop countermeasures and mitigation options include:

1. Identify countermeasure or mitigation options
2. Estimate the efficacy of mitigation options in reducing risks for specific asset-threat combinations
3. Develop a Scope of Work (SOW) for each option
4. Estimate costs of each option

Additional information regarding standards and guidelines for countermeasures and mitigation is provided in Section 5.

4.8.3 Assessing Countermeasures/Mitigation Options

Assessing countermeasures/mitigation options requires an estimate of costs, which can be determined by SMEs, and an estimate of benefits, which can be much more difficult to identify. To determine the efficacy of a specific mitigation option, it is important to assess:

- The ability of the mitigation measure to reduce consequences of a specific threat relative to a specific asset
- The ability of the mitigation measure to reduce the probability of the threat occurring
- The ability of the mitigation measure to reduce or eliminate the asset's vulnerability to the threat

The following asset-threat combination was used to create the example risk-reduction estimations shown in Table 4-11:

- Asset-Threat Combination: Baggage Claim Area/Armed Attack (large-hub airport)
- Total Risk: $32,314,444
- Mitigation Options:
    1. Control Case – Take no action
    2. Personnel/Procedures – Increase law enforcement presence and implement active shooter-specific procedures
    3. Physical Security – Institute physical security measures including increased video surveillance and video analytics

Given the risk estimation for this asset-threat combination, mitigation measures that reduce risk should be considered.

Estimations of risk reduction potential for mitigation measures should be arrived at in consultation with local law enforcement and security personnel, operations personnel, and engineers with mitigation experience. Event trees used in estimating vulnerability, such as the example provided in Appendix D5, may support estimates of risk reduction potential.

Table 4-8. Example: Estimates of Project Benefits

Project/Attributes	Option Benefit	Estimated Risk Reduction
Option 1 – Take no action		
	None	0%
Option 2 – Personnel and Procedures		
Hire five additional law enforcement officers to increase patrols in baggage claim and other public areas	Reduces vulnerability to an active shooter incident through increased presence of law enforcement; decrease response time	50%
Develop an active shooter plan to support specific response actions and to reduce threat impact	Reduces or eliminates the number of deaths and injuries, increase recovery capacities, and increase resiliency	6%
Conduct training and exercises (six 4-hour blocks of training, one tabletop exercise, and four drills)	Increases deterrence, detection, response and recovery capabilities via incident-specific procedures and training	6%
Plan maintenance/refresher training and exercises	Increases resiliency and maintains site- and incident-specific procedures based on evolving conditions; maintains preparedness through training/exercising	3%
Total Risk Reduction for Option 2		**65%**
Option 3 – Physical Security		
Video Surveillance – Provide fixed thermal cameras with video analytics	Decreases vulnerability to intruder entry; increases resiliency to responding to unauthorized entry	3%
Provide intercom/phone station at two additional areas near the baggage claim area; it may be tied to an existing phone switch or be a standalone system	Decreases vulnerability to unauthorized intruders	3%
Upgrade existing video surveillance headend and recording hardware/ software to support additional cameras	Supports more effective video surveillance	3%
Provide video surveillance monitoring station to include a client workstation, two 42-inch flat screen monitors, one 24-inch monitor, and one console	Increases detection and response capabilities to unauthorized entry	6%
Provide/upgrade network connectivity for video surveillance system, wired and wireless, as required	Supports more effective video surveillance	3%
Acquire and implement video analytic software	Supports more effective detection and response to video surveillance	6%
Execute camera maintenance and repair annual contract	Ensures availability of effective video surveillance and increases useful life	3%
Total Risk Reduction for Option 3		**28%**

As indicated, Options 2 and 3 are estimated to be 65% and 28% effective, respectively, in reducing risk. Additional information regarding evaluation of mitigation projects and lifecycle planning is provided in

Section 6, Benefit/Cost Analysis, and provides a more thorough approach to analyzing multi-year impacts of mitigation measures.

4.8.4 Managing, Monitoring, and Evaluating Selected Options

Managing, monitoring, and evaluating selected options supports management decisions and allocation of resources, with the intent of reducing risks against critical assets. Steps to achieve effective management of risk over time include, but are not limited to, the following:

- Set timelines for re-evaluation of mitigation measures
- Ensure that mitigation measures are properly maintained over time
- Monitor risk analysis inputs and collect new information
- Maintain and update the SVA to be consistent with existing conditions
- Evaluate the impact of changes on previous decisions used in the SVA
- Survey trends and intelligence data to identify necessary changes relative to specific critical assets and in the overall airport security posture

4.8.5 Periodic Security Vulnerability/Risk Assessment

Periodic vulnerability and risk assessment is a vital function in facilitating effective risk management. Assessment is recommended at least every five years and under the following circumstances:

- **Construction Projects** – Prior to and following major construction projects, identify potential impacts to existing mitigation measures and/or determine if additional risk is assumed as a result of new physical infrastructure
- **Modifications to Technology** – In response to changes in technology, identify potential impacts to existing countermeasures and/or determine if additional risk is assumed as a result of new changes in technology
- **Incidental Response** – If an incident occurs that was previously unforeseen or defeated existing countermeasures, identify more effective countermeasures to prevent recurrence
- **Procedural Modifications** – If plans or procedures are modified, identify whether modifications reduce the effectiveness of existing countermeasures and/or introduce new threats
- **Threat Posture** – If changes in threat posture become known via intelligence or other information sources, identify whether existing mitigation measures are effective in countering emerging threats

Periodic reassessment of risks and vulnerabilities facilitates mitigation measures that evolve with changing conditions.

SECTION 5: SECURITY MITIGATION ACTION PLANNING

As indicated in Section 4.8.2, Developing Countermeasures and Mitigation Options, many government and consensus-based guidelines and standards provide implementation and performance criteria to effectively mitigate specific types of risk. This section briefly examines some of those standards that can be referenced when developing performance guidelines to support effective mitigation. While not exhaustive, the standards and guidelines described herein provide examples to assist in identifying, planning, and implementing mitigation options. It is important to note that many standards and guidelines change frequently. Therefore, it is important to ensure use of the latest version or the version that may be legally binding relative to jurisdiction.[11]

Sections below focus on physical security, security technology, and processes and procedures to mitigate risk. For each category, examples of relevant sources of standards are provided that may help define mitigation projects. It is important that airports work through the entire SVA process and utilize the SVA team to define security performance criteria that are in line with existing resources, site-specific conditions, and senior leadership goals.

5.1 Mitigation Planning Team Members

Section 3, Key Success Factors for SVAs, provides recommendations regarding experts and stakeholders who may have a role in supporting an effective SVA process. Security mitigation action planning to address SVA findings is an area that is likely to require specific expertise. A non-exhaustive list of potential mitigation planning team members is indicated below:

- **ARFF** – Assistance in applicable codes and compliance advice
- Contracts and Administration – Assistance in sourcing products and services, developing scopes of work, and cost estimation
- **Dispatch/Communications/Control Center(s)** – Assistance in system coordination planning
- **Emergency Management/Emergency Planning** – Assistance in modifying plans and procedures, as well as training and exercise needs
- **Engineering** – Assistance in identifying relevant codes and standards, and in developing scopes of work, feasibility studies, and cost estimation
- Information Technology – Assistance in system coordination planning, and in developing scopes of work, feasibility studies, and cost estimation
- **Law Enforcement** – Assistance in modification of plans and procedures, and assessing effectiveness of mitigation options
- **Operations (landside, airside, terminal)** – Assistance in modification of plans and procedures, and assessing feasibility and effectiveness of mitigation options
- **Security and Badging** – Assistance in modification of plans and procedures, assessing effectiveness of mitigation options, and compliance

These potential SVA project team members may have specific roles depending on the types of mitigation options under consideration.

[11] Some city, county, and state jurisdictions adopt codes by reference. Thus, some codes and standards may be legally binding by ordinance or statute. Consult local and state code enforcement agencies to ensure compliance.

5.2 Physical Security Mitigation Strategies

Codes, standards, and guides to support physical security mitigation generally focus on hazard-specific needs and control of entry. Examples below are presented in three distinct categories: 1) Anti-terrorism, physical security, and asset protection; 2) Ballistics and explosives; and 3) Chemical, Biological, and Radiological (CBR) agents. Developing performance criteria to address specific hypothetical threats and deficiencies in that may be identified during an SVA process may require subject matter expertise from professional engineers and other life-safety trained professionals.

5.2.1 Anti-Terrorism, Physical Security, and Asset Protection

This category represents a broad set of codes, standards, and guides to:

1. Harden assets and deter, detect, and defend against malevolent threats of all kinds, including terrorism
2. Create barriers to entry for those with ill-intent
3. Protect assets, including people, from the impact of malevolent threats

Issues addressed in this broad category include design of evacuation, rescue and recovery systems (elevators, escalators, emergency doors, etc.); specifications for construction materials such as security doors, and fire protection; and various other anti-terrorism design features. Potential sources of standards that may support development of mitigation strategies under this category include, but are not limited to, the following:

- American National Standards Institute (ANSI)
- ASTM International (formerly American Society for Testing and Materials)
- Department of Defense Unified Facilities Criteria
- FEMA Buildings and Infrastructure Protection Series
- National Fire Protection Association
- US Army Corps of Engineers, Protective Design Center

5.2.2 Ballistics and Explosives

Many standards also exist to support mitigating ballistic and explosive threats. A non-exhaustive list of standards sources is provided below:

- ASTM International
- General Services Administration
- Underwriters Laboratory
- US Army Corps of Engineers, Protective Design Center

5.2.3 Chemical, Biological, and Radiological Agents

Standards exist to support mitigating attacks using CBR agents. A non-exhaustive list of sources is provided below:

- American Society of Heating, Refrigerating, and Air Conditioning Engineers
- Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health
- FEMA Buildings and Infrastructure Protection Series

5.3 Security Technology Mitigation Strategies

Codes, standards, and guides to support mitigation through security technology generally focus on communications, detection, and surveillance. Much of the technology used to mitigate risks is distributed throughout an airport in order to provide situational awareness to a central control center (i.e., AOC, Security Operations Center [SOC], Emergency Operations Center [EOC], or a combination thereof), either via individual systems or through an integrated Physical Security Information Management (PSIM) system. A non-exhaustive list of sources for standards supporting mitigation through communications, security, and situational awareness technologies is provided below:

- ANSI/Telecommunications Industry Association
- Building Industry Consulting Service International
- Department of Defense, Unified Facilities Criteria
- National Fire Protection Association
- National Public Safety Telecommunications Council
- Underwriters Laboratory

5.4 Process and Procedural Mitigation Strategies

Codes, standards, and guides to support mitigation through process and procedural modifications focus on response capabilities that are largely dependent on developing staff competencies to support various security functions under both normal and emergency conditions. FAA and TSA regulatory requirements for airport procedures are established and defined; references provided below are intended to build on those requirements to support mitigation of threats that are not specifically addressed in regulatory requirements. Moreover, the non-airport/aviation federal guides referenced herein are valuable in developing effective coordination strategies with outside agencies that may respond to airports during emergencies. A non-exhaustive list of standards supporting mitigation through processes and procedures is provided below:

- ACRP Report 74, Application of Enterprise Risk Management at Airports. Airport Cooperative Research Program, National Academy of Sciences, 2012
- ACRP Report 112, Airport Terminal Incident Response Planning, Airport Cooperative Research Program. National Academy of Sciences, 2014
- FEMA Comprehensive Preparedness Guide (CPG)101, Developing and Maintaining Emergency Operations Plans, U.S. DHS, November 2010
- FEMA CPG 502, Considerations for Fusion Center and Emergency Operations Center Coordination, U.S. DHS, September 2009
- Guidance on Planning for Integration of Functional Needs Support Services in General Population Shelters, U.S. DHS, November 2010
- Homeland Security Exercise and Evaluation Program (HSEEP), U.S. DHS, April 2013
- National Disaster Recovery Framework (NDRF), U.S. DHS, June 2016
- National Incident Management System (NIMS), U.S. DHS, 2008
- National Infrastructure Protection Plan (NIPP), U.S. DHS, 2013
- National Mitigation Framework, U.S. DHS, June 2016
- National Prevention Framework, U.S. DHS, June 2016
- National Response Framework, U.S. DHS, June 2016
- Public Area Security National Framework (PASNF). U.S. DHS, May 2017

5.5 Implementation Planning

Ideally, codes and standards allow development of performance criteria that support: 1) writing specifications; 2) vendor procurement; and 3) developing/installing, commissioning, and implementing mitigation measures. Procurement for infrastructure improvements and technology can take several months, and is highly dependent on existing rules and regulations governing procurement. Additional considerations that will impact the timeline for implementing mitigation measures are provided below:

PHYSICAL SECURITY AND TECHNOLOGY

- **Specification Development** – For physical security/technology, specifications will be required for procurement based on standards and desired performance criteria
- **Procurement** – For physical security/technology, procurement involves identifying relevant vendors, evaluating products in relation to standards and desired performance criteria, and contracting and delivery
- **Construction/Installation** – For physical security/technology, construction/installation is required and should be monitored to ensure proper functionality in relation to standards and performance criteria
- **Commissioning** – Prior to "going live" with infrastructure and/or technology improvements, allow one to three months to accommodate testing security systems or protective design elements
- **Staff Training/Exercises** – New security technology systems/protective design elements will also require staff training and exercising regarding proper use and maintenance of systems/elements. If new systems/elements require new staffing, additional time is necessary for hiring, on-boarding, and training/exercising
- **Adjustments/Implementation** – Final adjustments and implementation should be performed based on lessons learned via commissioning, training, and exercises
- **Complex Systems** – Allow additional time for implementing complex systems such as a PSIM; complex systems that address critical operations and threats should be evaluated under various adverse conditions prior to full operational use.

MODIFICATION/DEVELOPMENT OF SECURITY PLANS/PROCEDURES

- **RFP** – An RFP may be used to obtain a contractor to support plan/procedural development. The timeline for RFP development varies, and may take up to six months.
- **Procurement** – Once a vendor is chosen through the RFP process, contracting and other procurement functions may require two months or more.
- **Development/Modification of Plans/Procedures** – Modifications to plans and procedures generally requires airport stakeholder collaboration and may require six to twelve months.
- **Staff Training/Exercises** – Modifications to plans and procedures also require staff training and exercising of those assigned to implement and work within those plans and procedures.
- **Adjustments/Implementation** – Final adjustments to plans/procedures should be performed based on lessons-learned training and exercises.
- **Complex/New Plans** – Complex modifications or development of new plans/procedures may require up to twelve months for development, testing, and personnel training and exercises.

Mitigation options developed with a high degree of accuracy with respect to cost and effectiveness allow for informed decision-making using Benefit/Cost Analysis, which is described in Section 6.

SECTION 6: BENEFIT/COST ANALYSIS

Once mitigation options are identified, a benefit/cost analysis (BCA) is helpful to assist in management decisions regarding the most cost-effective mitigation options to implement. BCA provides estimates of anticipated benefits from a project over a specified period and compares them to the projected costs. Costs include resources required to develop and maintain the project over its useful life. Estimated benefits are based on the projected financial impacts of the project as related to risk mitigation.

FEMA[12] and the U.S. Department of Transportation[13] have each developed guidance to support effective BCA development and use for mitigation projects. This section incorporates relevant information from those guidance documents to:

- Describe an acceptable framework for preparing BCAs for mitigation projects
- Identify common data sources, values of key parameters, and additional reference materials for various BCA inputs
- Provide example calculations of the quantitative elements of a BCA

To be effective decision-making tools, BCAs should be performed for each proposed project to mitigate risk for a specific asset-threat combination. Generally, the baseline or control model for each asset-threat combination is a "No Action" option to mitigate the risk. Using the same scenario presented in Section 4.8.3, Assessing Countermeasures/Mitigation Options, a general example and process for conducting BCAs is provided below:

- Asset-Threat Combination: Baggage Claim Area / Armed Attack (large-hub airport)
- Total Risk: $32,314,444
- Options:
    1. Control Case – Take no action
    2. Personnel/Procedures – Increase law enforcement presence and implement active shooter-specific procedures
    3. Physical Security – Institute physical security measures including increased video surveillance and video analytics

The first step in the BCA process is identifying a conceptual scope of work for each project as described in Section 6.1 below.

6.1 Scope of Work

To facilitate an effective BCA, a SOW should be developed for each project to describe the general purpose and resources necessary to implement and maintain the project. In addition, it should address the timeline for completion, location of the project, and justify the importance of the project. The SOW should provide specific details about the proposed project including quantified resources and anticipated benefits the project will convey.

The SVA team should quantify and monetize all potential benefits and costs of a project. In addition, a schedule or timeline should be included to enable effective planning, and to identify any feasibility issues with each project.

[12] Benefit/Cost Analysis Reference Guide, Federal Emergency Management Agency Department of Homeland Security, June 2009.
[13] Benefit/Cost Analysis Guidance for Discretionary Grant Programs, U.S. Department of Transportation, December 2018.

Using the example described above, sample SOWs are provided below in Table 6-1:

Table 6-1. Scopes of Work for Proposed Mitigation Projects

Project/Attributes	Description
Option 1 – Take no action	
None	
Option 2 – Personnel/Procedures	
Project Purpose	Increase law enforcement presence and implement active shooter-specific procedures to improve deterrence, detection, defense, response and recovery capabilities.
Resources	• Five additional law enforcement officers to increase patrols in baggage claim and other public areas • Develop a threat-specific (active shooter) plan • Conduct training and exercises (six 4-hour blocks of training, one tabletop exercise, and four drills) • Implement activities to maintain the active shooter plan through annual review, training, and exercises
Timeline for Completion	Initial hiring, planning, training and exercising – six months
Project Location	Baggage Claim / Public Areas
Project Importance	Potentially critical project to reduce risks associated with an active shooter pending analysis of benefits and costs.
Option 3 – Physical Security	
Project Purpose	Implement physical security measures to improve deterrence, detection, defense, response and recovery capabilities.
Resources	• Video surveillance – Fixed thermal cameras with video analytics • Provide intercom/phone station at two additional areas near the baggage claim area • Upgrade existing video surveillance headend and recording hardware/software to support additional cameras • Provide video surveillance monitoring station to include a client workstation, two 42-inch flat screen monitors, one 24-inch monitor, and one console • Provide/upgrade network connectivity for video surveillance system, both wired and wireless, as required • Acquire and implement video analytics software • Execute a camera maintenance and repair annual contract
Timeline for Completion	Less than six months
Project Location	Baggage Claim / Public Areas
Project Importance	Potentially critical project to reduce risks associated with an active shooter pending analysis of benefits and costs.

With a general SOW for each of the proposed mitigation projects, the next step is to identify and quantify the potential benefits.

6.2 Identifying Potential Benefits

As indicated in the example above, the risk estimate for an armed attack in a baggage claim area is $32,314,444. This estimate is premised on assumptions relating to the consequences of such an attack. Estimates of risk reduction potential, or benefits, of each project are required to conduct a BCA. While developing monetary estimates of benefits is rarely an exact science, estimates can be made based on the following questions:

1. Does the project reduce the consequences of a threat on a specific asset? An example is blast-resistance construction, which reduces the consequences of an explosive device
2. Does the project decrease the probability of a threat occurring? Examples include measures that improve deterrence and/or detection of malevolent threats, such as video surveillance and screening
3. Does the project reduce the vulnerability of an asset against a specific threat? Examples include access control and other barriers to entry

Examples of project benefits and associated monetary estimates are provided in Table 6-2.

Table 6-2. Estimates of Project Benefits

Project/Attributes	Option Benefit	Monetized Benefit
Option 1 – Take no action		
None	None	$0
Option 2 – Personnel and Procedures		
Hire five additional law enforcement officers to increase patrols in baggage claim and other public areas.	Reduces vulnerability to an active shooter incident through increased presence of law enforcement; decreases response time.	$16,000,000
Develop an active shooter plan to support specific response actions and to reduce threat impact.	Reduces or eliminates the number of deaths and injuries, increases recovery capacities, and increases resiliency.	$2,000,000
Conduct training and exercises (six 4-hour blocks of training, one tabletop exercise, and four drills).	Increases deterrence, detection, response and recovery capabilities via incident-specific procedures and training.	$2,000,000
Extended cost for active shooter plan and training (review and update every year and one operational exercise annually).	Increases resiliency and maintains site- and incident-specific procedures based on evolving conditions; maintains preparedness through training/exercising.	$1,000,000
Total Monetized Benefit for Option 2		**$21,000,000**
Option 3 – Physical Security		
Video Surveillance – Provide fixed thermal cameras with video analytics.	Decreases vulnerability to intruder entry; increases resiliency to responding to unauthorized entry.	$1,000,000
Provide intercom/phone station at two additional areas near the baggage claim area. It may be tied to an existing phone switch or as a standalone system.	Decreases vulnerability to unauthorized intruders.	$1,000,000
Upgrade existing video surveillance headend and recording hardware/ software to support additional cameras.	Supports more effective video surveillance.	$1,000,000

Project/Attributes	Option Benefit	Monetized Benefit
Provide video surveillance monitoring station to include a client workstation, two 42-inch flat screen monitors, one 24-inch monitor, and one console.	Increases detection and response capabilities to unauthorized entry	$2,000,000
Provide/upgrade network connectivity for video surveillance system, wired and wireless, as required.	Supports more effective video surveillance.	$1,000,000
Acquire and implement video analytics software.	Provides program for video analytics/ to cameras for detection and response.	$2,000,000
Execute camera maintenance and repair annual contract.	Ensures availability of effective video surveillance and increases useful life.	$1,000,000
Total Monetized Benefit for Option 3		**$9,000,000**

Having identified estimates of benefits for each option, the next step is to identify project costs.

6.3 Identifying Project Costs

The project cost estimate should provide costs for overall project development and should itemize specific costs by task or resource including physical assets, contractor costs, and management fees. To the extent possible, all costs should be documented and should meet the following criteria:

- Identify the useful life of the project (See Appendix F, Table F-1, Project Useful Life Estimates)
- Identify one-time and repetitive costs
- Provide a breakdown of project costs including materials, labor, and fees corresponding to individual SOW activities
- Identify contractor costs
- Identify management costs
- Identify post-implementation maintenance costs throughout the project useful life
- Documents sources for estimated costs
- Provide a detailed budget narrative

Continuing with the *Baggage Claim Area / Armed Attack* example, Table 6-3 identifies estimated costs. For demonstration purposes, the life cycles of both Options 2 and 3 are ten years.

Table 6-3. Estimates of Project Costs

Project	Cost Type	Cost
Option 1 – Take no action		
None	None	$0
Option 2 – Personnel and Procedures		
Hire five additional law enforcement officers to increase patrols in baggage claim and other public areas.	Annual	$750,000
Develop an active shooter plan to support specific response actions and to reduce threat impact.	One-time cost	$200,000
Conduct training and exercises (6, 4-hour blocks of training, one tabletop exercise, and 4 drills).	One-time cost	$190,000

Project	Cost Type	Cost
Extended cost for active shooter plan and training (review and update plan and perform one operational exercise annually).	Annual	$85,000
Option 3 – Physical Security		
Video Surveillance – Provide fixed thermal cameras with video analytics.	One-time cost	$1,000,000
Provide intercom/phone station at two additional areas near the baggage claim area; tie to an existing phone switch or as a standalone system.	One-time cost	$1,000,000
Upgrade existing video surveillance headend and recording hardware/ software to support additional cameras.	One-time cost	$1,000,000
Provide video surveillance monitoring station to include a client workstation, two 42-inch flat screen monitors, one 24-inch monitor, and one console.	One-time cost	$2,000,000
Provide/upgrade network connectivity for video surveillance system, wired and wireless, as required.	One-time cost	$1,000,000
Acquire and implement video analytics software.	One-time cost	$2,000,000
Execute camera maintenance and repair annual contract.	Annual	$1,000,000

6.4 Life Cycle Estimates of Benefits and Costs

Developing an accurate BCA requires life cycle estimates of benefits and project costs. In addition to identifying the life cycle, one-time, and recurring costs throughout the useful life of the project, a discount rate should be identified to develop net-present-value calculations for benefits and costs. Appendix F, Table F-2 identifies a standard discount rate of 7%. Using this discount rate, net present value (NPV) benefits and costs can be calculated throughout the life cycle using the following equation:

$$NPV = \frac{FV}{(1+i)^t}$$

Where NPV = Net Present Value of Benefit/Cost

FV = Future value of payment in real dollars

i = Real discount rate (7%)

t = Years in the future of payment/benefit where base year of analysis is t = 0

6.4.1 Net Present Value – Benefits

Using the equation above, Table 6-4 discounts benefits over the useful life of the projects using a discount rate (i) of 7% and a life cycle (t) of 0–10 years. In this case, the total benefit (calculated in Table 6-2) is divided over the life cycle ($21,000,000/10 = $2,100,000 for Option 2 and $9,000,000/10 = $900,000 for Option 3).

Table 6-4. Net Present Value of Benefits

Year	Option 1 – Take no action	Option 2 – Personnel and Procedures	Option 3 – Physical Security
2019	$0	$2,100,000	$900,000
2020	$0	$1,962,617	$841,121

Year	Option 1 – Take no action	Option 2 – Personnel and Procedures	Option 3 – Physical Security
2021	$0	$1,834,221	$786,095
2022	$0	$1,714,226	$734,668
2023	$0	$1,602,080	$686,606
2024	$0	$1,497,271	$641,688
2025	$0	$1,399,319	$599,708
2026	$0	$1,307,774	$560,475
2027	$0	$1,222,219	$523,808
2028	$0	$1,142,261	$489,540
2029	$0	$1,067,534	$457,514
Total NPV Benefits	**$0**	**$16,849,521**	**$7,221,223**

6.4.2 Net Present Value – Costs

In Table 6-5, the NPV equation is applied to annual costs for Options 2 and 3 (calculated in Table 6-3).

Table 6-5. Net Present Value of Annual Costs

Year	Option 2 – Personnel and Procedures		Option 3 – Physical Security
	LEO Salaries	Annual Program Review	Maintenance Contract
2019	$750,000	$85,000	$200,000
2020	$700,935	$79,439	$186,916
2021	$655,079	$74,242	$174,688
2022	$612,223	$69,385	$163,260
2023	$572,171	$64,846	$152,579
2024	$534,740	$60,604	$142,597
2025	$499,757	$56,639	$133,268
2026	$467,062	$52,934	$124,550
2027	$436,507	$49,471	$116,402
2028	$407,950	$46,234	$108,787
2029	$381,262	$43,210	$101,670
Total NPV Costs	**$6,017,686**	**$682,004**	**$1,604,716**

Table 6-6 indicates the total cost for Options 2 and 3, including the annualized NPV costs in Table 6-5 as well as the one-time costs.

Table 6-6. Net Present Value of Total Costs

Option/Attributes	Cost Type	Cost
Option 2 – Increase Law Enforcement Presence and Procedural Security Measures		
Hire five additional law enforcement officers to increase patrols in baggage claim and other public areas	Annual	$6,017,686
Develop a threat-specific (active shooter) plan	One-time cost	$200,000
Conduct training and exercises (6, 4-hour blocks of training, one tabletop exercise, and 4 drills)	One-time cost	$190,000
Extended cost for active shooter plan, training, and exercises (annual review and operational exercise)	Annual	$682,004
Total NPV Cost for Option 2		**$7,089,691**
Option 3 – Institute Physical Security Measures		
Video surveillance – Provide fixed thermal cameras with video analytics	One-time cost	$200,000
Provide intercom/phone station at two additional areas near the baggage claim area	One-time cost	$5,000
Upgrade existing video surveillance headend and recording hardware/software to support additional cameras	One-time cost	$30,000
Provide video surveillance monitoring station to include a client workstation, two 42-inch flat screen monitors, one 24-inch monitor, and one console	One-time cost	$12,500
Provide/upgrade network connectivity for video surveillance system, both wired and wireless, as required	One-time cost	$30,000
Acquire and implement video analytics software	One-time cost	$20,000
Camera maintenance and repair annual contract	Annual	$1,604,716
Total NPV Cost for Option 3		**$1,902,216**

Having estimated NPV benefits and costs for projects, the benefit/cost ratio can be calculated as indicated in Section 6.5 below.

6.5 Benefit/Cost Ratio

The benefit/cost ratio (BCR) is calculated using the equation:

$$\text{BCR} = \frac{\text{NPV (Benefit)} - \text{NPV (Cost)}}{\text{NPV (Cost)}} \times 100$$

Using this equation, the BCRs for Options 2 and 3 are provided in Table 6-7.

Table 6-7. Benefit/Cost Ratio Calculations

Parameter	Option 1 – Take no action	Option 2 – Personnel and Procedures	Option 3 – Physical Security	Implement Options 2 & 3
NPV-Cost	$0	$7,089,691	$1,902,216	$8,991,907
NPV-Benefit	$0	$16,849,521	$7,221,223	$24,070,744
BCR	NA	138%	280%	168%

In some cases, mitigation projects are mutually exclusive. In other cases, multiple mitigation projects can be implemented to reduce risk. If two or more projects offer unique benefits and have a positive benefit/cost ratio, it may be prudent to implement multiple projects assuming that budget is available. If fiscal resources are limited, the project with the highest benefit/cost ratio should be implemented. As indicated in Table 6-7, Options 2 and 3 both provide a positive BCR, individually and in combination.

6.6 Decision-Making Process

The BCR provides important information to support decision-making regarding risk mitigation projects. Other factors, such as budgetary constraints, may override use of the BCR as a determinant. Thus, it is important to maintain alternatives identified during the scope of work process, particularly those of lower cost.

Engineering and operational feasibility may also be determinants in the ability to implement a project and the project type dictates the level of engineering support needed. Mitigation projects that involve construction generally require risk data and past performance data. Other information that supports engineering review includes:

- Codes and regulations
- Engineering performance criteria
- Project-specific design information

Additional BCA Data Sources are provided in Appendix F. To document the entire SVA process, an Airport SVA Report Template is attached as Appendix G. This template can be used to document the entire process from Step 1, project chartering, through BCA and implementation of mitigation measures.

REFERENCES

A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection. National Cooperative Highway Research Program Project 20-07/Task 151B, Science Applications International Corporation, May 2002.

Aviation Safety Manual. International Civil Aviation Organization, Doc 9859 AN/474, Third Edition, 2013.

Aviation Security Manual. International Civil Aviation Organization, Doc 8973/8, Eighth Edition, 2011.

Bayne, James. An Overview of Threat and Risk Assessment. SANS Institute, 2002.

Benefit/Cost Analysis Guidance for Discretionary Grant Programs, U.S. Department of Transportation, December 2018.

Benefit/Cost Analysis Reference Guide, Federal Emergency Management Agency Department of Homeland Security, June 2009.

Blass, Deborah. PARAS 0014: Blast Mitigation Strategies for Non-Secure Areas at Airports. Arup USA, Inc., Safe Skies, August 2018.

Chief Security Officer Guideline, ASIS International, 2008.

CIP-014-2 – Physical Security, Critical Infrastructure Protection (CIP), North American Electric Reliability Corporation (NERC), October 2, 2015.

Comprehensive Preparedness Guide 101, Developing and Maintaining Emergency Operations Plans. Federal Emergency Management Agency, U.S. Department of Homeland Security, November 2010.

Comprehensive Preparedness Guide 201, Threat and Hazard Identification and Risk Assessment Guide. Department of Homeland Security, Second Edition, August 2013.

Comprehensive Preparedness Guide 502, Considerations for Fusion Center and Emergency Operations Center Coordination. Federal Emergency Management Agency, U.S. Department of Homeland Security, September 2009.

Emergency Response Planning for Military Water Systems. U.S. Army Center for Health Promotion and Preventative Medicine, Water Supply Management Program, Technical Guide 297, April 2005.

Flamenbaum, Harold, et al. PARAS 0006: Employee Inspections Synthesis Report. Faith Group, LLC, Safe Skies, February 2017.

General Security Risk Assessment Guideline. ASIS International, 2003.

Guide for Developing High Quality Emergency Operations Plans for Institutions of High Educations. U.S. Department of Education, Office of Elementary and Secondary Education, Office of Safe and Healthy Students, June 2013.

Guide for Developing High Quality School Emergency Operations Plans. U.S. Department of Education, Office of Elementary and Secondary Education, Office of Safe and Healthy Students, June 2013.

Guidelines and Model for Analyzing the Vulnerability of Chemical Sites. Synthetic Organic Chemical Manufacturers Association, August 16, 2002.

Homeland Security Exercise and Evaluation Program. U.S. Department of Homeland Security, April 2013.

Information Circular IC 15-01E, Insider Threat. U.S. Department of Homeland Security, Transportation Security Administration, August 30, 2018.

Jaeger, Calvin D., et al. Development of an Automated Security Risk Assessment Methodology Tool for Critical Infrastructures. Sandia National Laboratories, SAND2008-81438143, December 2008.

Landside Security Handbook. Airports Council International, First Edition, 2018.

Lehocky, Stephen, et al. PARAS 0008: Findings and Practices in Sharing Sensitive Information. TransSolutions, LLC, Safe Skies, February 2017.

Maritime Security: Elements of an Analytical Framework for Compliance Measurement and Risk Assessment, United Nations, UNCTAD/SDTE/TLB/2005/4, 2006.

National Disaster Recovery Framework. U.S. Department of Homeland Security, June 2016.

National Incident Management System. U.S. Department of Homeland Security, 2017.

National Infrastructure Protection Plan. U.S. Department of Homeland Security, 2013.

National Mitigation Framework. U.S. Department of Homeland Security, June 2016.

National Preparedness Goal. Second Edition. U.S. Department of Homeland Security, September 2015.

National Prevention Framework. U.S. Department of Homeland Security, June 2016.

National Resilience Framework. U.S. Department of Homeland Security, June 2016.

National Response Framework. U.S. Department of Homeland Security, June 2016.

PARAS 0004: Recommended Security Guidelines for Airport Planning, Design, and Construction. TranSecure, Inc., Safe Skies, April 2017.

PARAS 0007: Quick Guide for Airport Cybersecurity. Synergy Solutions, Inc., Safe Skies, January 2018.

PARAS 0010: Guidance for Protecting Access to Vital Systems Impacting Airport Security. Faith Group, LLC, Safe Skies, October 2017.

Pipeline Security Guidelines. U.S. Department of Homeland Security, Transportation Security Administration, March 2018.

Pipeline Security Smart Practices. U.S. Department of Homeland Security, Transportation Security Administration, Pipeline Security Transportation Sector Network Management, August 2006.

Public Area Security National Framework. U.S. Department of Homeland Security, May 2017.

Recommended Security Guidelines for Airport Planning, Design, and Construction, U.S. Department of Homeland Security, Transportation Security Administration, May 1, 2011.

Report 112, Airport Terminal Incident Response Planning, Airport Cooperative Research Program. National Academy of Sciences, 2014.

Report 74, Application of Enterprise Risk Management at Airports. Airport Cooperative Research Program, National Academy of Sciences, 2012.

Rieder, Jr., Rene, et al. PARAS 0009: Guidance for Security Management Systems. Arup USA, Inc., Safe Skies, March 2018.

Risk Analysis and Management for Critical Asset Protection, American National Standards Institute (ANSI)/American Society of Mechanical Engineers (ASME)-Innovative Technologies Institute, LLC/American Water Works Association (AWWA), J100-10, First Edition, July 1, 2010.

Risk Assessment: A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings. Federal Emergency Management Agency, FEMA 452, January 2005.

Risk Context Statement. International Civil Aviation Organization, Aviation Security Panel Working Group on Threat and Risk, 2018.

Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-30, July 2002.

Rooney, James J. and Vanden Heuvel, Lee N. Root Cause Analysis for Beginners. Quality Progress, American Society for Quality, July 2004.

Security and Emergency Preparedness Action Items for Transit Agencies, A Resource Document for Transit Agencies. U.S. Department of Transportation, Federal Transit Administration, September 2014.

Security Management Standard: Physical Asset Protection, ASIS International, American National Standards Institute (ANSI)/ASIS Physical Asset Protection (PAP).1-2012.

Security Operations for Public Transit. American Public Transportation Association, SS-SIS-RP-012-13, March 26, 2013.

Security Planning for Public Transit. American Public Transportation Association, SS-SIS-RP-011-13, March 26, 2013.

Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries. American Petroleum Institute/National Petrochemical and Refiners Association, May 2003.

Site Security Guidelines for the U.S. Chemical Industry. American Chemistry Council, et al, October 2001.

Standard Practice for System Safety, Department of Defense, Military Standard 882D, February 10, 2000.

Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.3. National Counterintelligence and Security Center, Office of the Director of National Intelligence, IC Tech Spec-for ICD/ICS 705, September 10, 2015.

The Public Transportation System Security and Emergency Preparedness Planning Guide, U.S. Department of Transportation, Federal Transit Administration (FTA), DOT-FTA-MA-26-5019-03-01/ DOT-VNTSC-FTA-03-01, Final Report, January 2003.

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, 1st Edition, August 2013.

Title 14 Code of Federal Regulations, Part 139 – Certification of Airports, June 9, 2004.

Title 33 Code of Federal Regulations, Part 105 – Maritime Security: Facilities, July 1, 2003.

Title 49 Code of Federal Regulations, Part 1540 – Civil Aviation Security: General Rules, October 1, 2010.

Title 49 Code of Federal Regulations, Part 1542 – Airport Security, October 1, 2010.

Transit Agency Security and Emergency Management Protective Measures. Federal Transit Administration, Battelle TotalSecuirty.US Transportation Resource Associates, National Transit Institute, November 2006.

Transit Security Design Considerations. U.S. Department of Transportation, Federal Transit Administration, FTA-TRI-MA-26-7085-05/DOT-VNTSC-FTA-05-02, Final Report, November 2004.

Transit Security Update, Synthesis 80. Transit Cooperative Research Program, Transportation Research Board, Nakanishi Research and Consulting, LLC, 2008.

Transportation Security Guidelines for the U.S. Chemical Industry. American Chemistry Council, et al, 2001.

Willis, Henry H., et al. Estimating Terrorism Risk. Center for Terrorism Risk Management Policy. RAND Corporation, 2005.

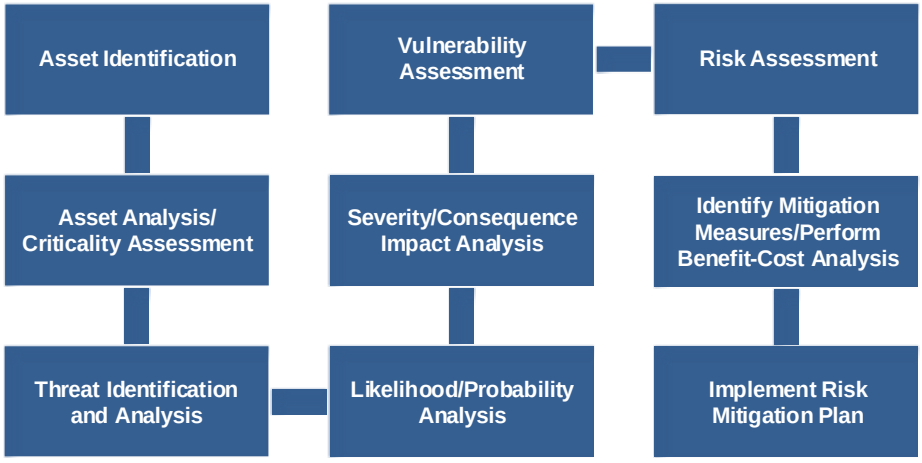
APPENDIX A: RESEARCH DATA

This appendix provides analysis of risk assessment literature and results of airport stakeholder outreach. Data provided herein was used to develop recommendations for conducting airport risk and security vulnerability assessments provided throughout this document.

A1 – Literature Review Summary

An exhaustive search of risk assessment information was conducted via review of academic research, security industry references, and various critical infrastructure sectors as defined in the NIPP. Risk assessment models developed for other types of critical infrastructure provide valuable information in developing an airport-specific methodology. In general, risk assessment processes across most of the literature reviewed follow the general process flow indicated in Figure A-1.

Figure A-1. General Process Flow for Assessing Risk



The desired result of this process in all of the assessment methodologies includes:

1. Determination of critical assets and their vulnerability based on their operational importance, level of protection, and redundancy
2. Determination of plausible threats
3. A list of prioritized risks associated with threats applied to specific assets (asset-threat combinations)
4. A list of necessary mitigation needs based on level of risk acceptance, plausibility of mitigation measures, and benefit/cost analysis
5. A risk mitigation plan to reduce risks to an acceptable level as defined by organizational leadership

Another similarity among most of the accepted risk and security vulnerability assessment methodologies is the inclusion of some form of a risk register to support prioritization of risk and, ultimately, mitigation measures, as exemplified in Table A-1.

Table A-1. Example Risk Register

Qualitative Risk Rating	Quantitative Risk Rating	Likelihood	Consequences	Vulnerability
Very High	>5	Imminent	Very high number of fatalities and injuries, and/or economic and operational impact	Very High
High	3-5	Expected	High number of fatalities and injuries, and economic and operational impact	High
Medium	2-3	Possible	Moderate number of fatalities and injuries, and economic and operational impact	Medium
Low	1-2	Possible	Low number of fatalities and injuries, and economic and operational impact	Low
Very Low	<1	Very negligible	Very low number of fatalities and injuries, and economic and operational impact	Very Low

Given the general conformity of process and prioritization among various risk and SVA methodologies, the literature was reviewed to identify notable differences that may be applicable to airport risk and security assessment. Differences in approach among various literary sources support development of an airport methodology focusing on three primary types of risk assessment:

1. Initial and routine periodic airport-wide risk assessment
2. Risk assessment in advance of a capital project to support design, construction, and commissioning
3. Risk assessment in response to a particular incident or occurrence at the airport or within the aviation sector (i.e., security incident, increased threat level due to intelligence, or natural hazard event).

The general process flow for assessing risk (Figure A-1, above) serves as a model for airport-specific SVA recommendations provided in this guidebook. Detailed results of the literature review are provided in Appendix B.

A2 – Stakeholder Outreach and Engagement

To augment the literature review, outreach was performed among airport stakeholders, aviation industry representatives, and other sectors to gather data and general information regarding the conduct of SVAs and similar assessments. Information gathered via stakeholder outreach is provided below.

A2.1 – Airport Outreach

Airport outreach was conducted through an online survey and through follow-up phone interviews with selected survey respondents. The online survey consisted of questions designed to elicit responses regarding each airport representative's experience in conducting SVAs internally and/or with TSA Joint Vulnerability Assessments (JVA). Twenty airport representatives responded from a variety of small, medium, and large hub airports.

Eighty-seven percent of all airports and 100% of medium and large hub airports surveyed had participated in a TSA JVA in the last 5 years. Phone interviews were conducted with three airport respondents to gather additional information about their experiences with both the JVA and internal airport authority-based SVAs. Phone interviews consisted of open-ended questions to allow participants to provide specific experience, insight, and lessons learned. These are summarized below.

A2.1.1 – SVA Initiation and Methodology

Of the 20 airports surveyed, 65% had conducted an internal SVA at their airport in the last five years. Seven of the airports surveyed utilized an outside contractor to conduct the SVA, while the remaining 13 airports partnered with local law enforcement, local TSA, and other airport stakeholders. SVAs were led most often by airport security, airport police, or airport operations personnel. Reasons cited for initiating an SVA varied, but most were initiated due to an accident, threat or incident, and/or airport construction/capital project.

Survey results revealed the need for an airport-specific methodology that can be used for any size of airport. Only two of the 20 airports surveyed utilized an existing standard for conducting SVAs. Eight airports used locally developed methods, questionnaires, and equations, and 10 reported that they did not know what type of methodology was used. Several survey participants indicated the need for guidance regarding:

1. Type of threats on which airports should focus
2. Long-term strategies for maintaining a relevant threat profile as threats evolve
3. Mitigation strategies

Tools and practices cited most frequently by interviewees as being useful in conducting SVAs include:

- Preliminary meetings with senior leadership
- Preliminary lists of threats/scenarios
- Checklists and templates for the SVA project manager
- Development of airport diagrams applicable to areas being assessed to scope the SVA and to identify potential interdependencies
- Small group discussions among relevant stakeholders
- Facilitated one-on-one interviews with participants

A2.1.2 – SVA/JVA Benefits and Airport Improvements

Airport respondents reported benefits in conducting an SVA, JVA, or both. Respondents generally indicated the need for airports to conduct at least partial or full operational assessments on an ongoing basis, and to treat the SVA/JVA as a living document to be updated as the airport physical environment and operations evolve. A majority of airports took action to implement changes as a result of the SVA/JVA. A summary of cited SVA/JVA benefits is provided below:

- The assessment was helpful in planning and prioritizing future security projects.
- The assessment was helpful in focusing priorities on activities/projects that have a high security benefit and low (or lower) cost.
- The JVA highlighted areas for improvement that the airport had already identified, which strengthened efforts to push projects forward for funding and execution. Projects included perimeter enhancements, additional camera coverage, modified police procedures, and increased police presence at the curb for traffic control and preventing unattended vehicles.
- The JVA helped justify security department business cases for capital projects planned for the next three to five years.
- The SVA provided background support and justification for projects, contracts, and other airport security initiatives.
- Data was used to review and update procedures, and to identify and develop security-related projects.

- The assessment led to researching current security technologies and to adding cameras at loading docks.
- Based on the JVA, the airport is now considering blast analysis
- The internal SVA identified necessary modifications to security policies and procedures.
- The SVA justified the need to add bollards, increase camera coverage, and consider different methods of perimeter fence protection

A2.1.3 – SVA Challenges

Airport representatives cited several challenges both in conducting an internal SVA and in implementing modifications as a result of the SVA as indicated below:

- Conflicting opinions about what constitutes a threat to the airport and/or what threats are relevant to address in the assessment
- Difficulty in scheduling meetings and interviews
- Financial/budget constraints
- Time required to initiate and conduct the SVA
- Difficulty in finding participants to provide relevant information and data
- Lack of support from senior leadership and management
- Conflicting opinions about what constitutes critical airport assets and targets
- Time and resources needed for continuous evaluation

A2.2 – Federal Outreach

Outreach was also conducted to federal agencies including TSA and the DHS Office of Infrastructure Protection.

A2.2.1 – TSA Joint Vulnerability Assessments

An interview of representatives from the TSA Federal Air Marshal Service, Security Assessments Section was conducted to obtain JVA program information, requirements, and a primer on execution of JVAs from a program-owner perspective. The interview provided insight regarding experiences of airports in participating in a JVA, as well as the intended outcomes from a programmatic perspective.

The TSA JVA program is a congressionally mandated program led by the Supervisory Federal Air Marshal. The current program objective is focused on assessing threats and vulnerabilities, including a variety of external and insider threat pathways at the largest domestic hub airports. Final JVA reports (non-punitive) are shared with FSDs to aid in mitigating identified vulnerabilities with airport stakeholders. The JVA is designed as a non-regulatory assessment to address the totality of each airport's circumstances. Features of the JVA include:

- A risk-based approach
- Evaluation of each airport independently with no comparison to other airports
- Conducted overtly with airport management awareness
- Identification of vulnerabilities or related issues "hiding in plain sight"
- No testing of alarms, response times, traditional regulatory issues, etc.
- Non-punitive, non-regulatory inspection conducted by airport Transportation Security Inspectors
- No fines, penalties, or fees associated with results

The schedule prioritization is based on airport size and criticality. Mandatory assessments are conducted for all 28 Category X airports, five Category I airports, and one Category II airport. JVAs will be

conducted on an ongoing basis, at least once every three to five years, at each mandatory airport. Other airports receive JVAs by request from the airport and/or in advance of a national special security event (e.g., Super Bowl, national conventions, etc.) Any airport-requested JVA is paid for through the local FSD budget. The annual fiscal year schedule for airports receiving JVAs is provided to the FSDs who, in turn, are directed to reach out to their respective airports to identify limitations and scheduling with the airport operator.

A typical JVA lasts four days and consists of two- to five-person teams depending on airport size. The process begins with an introductory briefing with the airport operator and key stakeholders. The JVA team then branches out across the airport to visually assess and photograph as many areas as possible, and to conduct interviews with airport employees and stakeholders. At the conclusion of the JVA, an outgoing briefing is provided to the airport operator to identify vulnerabilities, potential mitigation options, and recognized practices. A final report is prepared and released to the airport 60–90 days following the assessment and includes photographs and other evidence to support the JVA.

A2.2.2 – Office of Infrastructure Protection Assist Visits

The DHS Office of Infrastructure Protection Assist Visits are a cornerstone of the voluntary outreach effort to critical infrastructure owners and operators. An Assist Visit, conducted by Protective Security Advisors, is intended to accomplish the following:

- Establish and enhance the DHS relationship with critical infrastructure owners and operators
- Inform critical infrastructure owners and operators of the importance of their facility
- Explain how their facility or service fits into its specific critical infrastructure sector
- Provide an overview of the resources available to the facility to enhance security resilience
- Reinforce the need for continued vigilance and cooperation with stakeholders

While it is not apparent that Assist Visits are widely used within airports, they do provide an additional resource from which an outside perspective regarding critical infrastructure protection can be gained.

A2.3 – Other Sector Outreach

Interviews were conducted with three representatives who have significant risk assessment experience in the chemical, transportation systems, and water sectors. Interviewees were asked to describe various methodologies used within those sectors and to identify recommendations that would improve their usability and efficacy.

Interviewees noted using guidance described in the Literature Review to conduct risk assessment in the transportation and water sectors (see Appendix B, Sections B4.7 and B4.8, respectively). In the chemical sector, a methodology known as CARVER was cited as an additional assessment methodology.

Developed by the United States Army, CARVER is a targeting prioritization tool that has been adapted for use in other industries including law enforcement and IT. CARVER is an acronym for the following six attributes:[14]

- Criticality – Determination of importance of the node (or asset) is to the mission
- Accessibility – Ability of an adversary to physically access and egress from target
- Recuperability – Ability of system to recover from an attack

[14] Vulnerability Assessment Method Pocket Guide, A Tool for Center of Gravity Analysis, Rand Corporation, Arroyo Center, ISBN 978-0-8330-8689-1, 2014.

- Vulnerability – Ease of accomplishing attack
- Effect – Amount of direct loss from an attack
- Recognizability – Ease of identifying target

In discussing sector-specific methodologies and other more general methodologies, all interviewees agreed that risk is ultimately a function of consequence, threat probability, and asset vulnerability. While methodologies may approach assessment differently, the three primary functions of risk are the same when applied to a specific asset and threat. The J100 and CARVER methodologies are contrasted in Table A-2. While CARVER has similar features, J100 treats threat characterization and probability in the water sector in a manner that is needed in airports.

Table A-2. Methodology Comparison

AWWA J100 Standard	CARVER
Asset Characterization	Recuperability (an aspect of Asset Characterization)
Threat Characterization	(threats defined in military terms)
Consequence Analysis	Criticality and Effect
Vulnerability Analysis	Accessibility, Recognizability, and Vulnerability
Threat Analysis	(performed as a function of threat identification)

Another issue identified by interviewees is training. Similar to this guidebook, each methodology is described in a manual intended to guide the user through a sector-specific SVA. However, interviewees pointed out that, in addition to a manual, each of the methodologies has a corresponding training course to provide competency-based learning in how to properly conduct an SVA. Two of three interviewees recommended against conducting an SVA without formal training. Options suggested by interviewees include:

- Seek direct assistance to conduct an SVA from local emergency management agencies (city/county/state) from officials with formalized training
- Work with local (city/county/state) emergency management agencies to identify relevant risk assessment training
- In lieu of a comprehensive SVA, consider using risk screening tools initially to identify assets and threats of the highest concern, and augment with outside assistance for further assessment of critical assets and threats. DHS's *Integrated Rapid Visual Screening of Buildings*[15] may serve as a valuable screening tool

Interviewees also described difficulties in gaining consensus regarding quantitative estimates of probability and vulnerability. Probability and vulnerability are important as a means to rank asset-threat combinations relative to each other to assist in prioritizing them. If determining quantitative estimates for either of these parameters is challenging, it may be advisable to use qualitative categories (high, medium, low).

Recommendations provided by interviewees to overcome obstacles to conducting SVAs are provided below:

[15] Building and Infrastructure Protection Series, Integrated Rapid Visual Screening of Buildings, BIPS 04, Department of Homeland Security, Science and Technology, September 2011.

1. To the extent feasible, use local SMEs to gain consensus regarding probability for various malevolent threats.
2. Err on the side of simplicity; while numeric estimations of risk may be desirable, if numeric estimations of probability and vulnerability are difficult to determine, use qualitative categories.
3. To the extent feasible, quantify consequences using best practices and SMEs. Consequence estimations support decision-making regarding mitigation measures and allow benefit/cost analysis to be conducted.
4. Eliminate low probability threats and invulnerable assets from the assessment.
5. Use of any methodology without formally trained personnel on the SVA project team is likely to hinder the process.

Challenges and recommended SVA strategies identified during stakeholder outreach are used in developing the airport-specific SVA methodology provided in this guidebook.

APPENDIX B: LITERATURE REVIEW

This appendix provides a detailed literature review that was used to inform development of the airport-specific SVA methodology described in this guidebook.

B1 – Broad Government Doctrine

DHS and many other federal agencies have worked collaboratively to develop guidance documents to facilitate security, preparedness, and resiliency throughout the nation. With noted exceptions, most of these guidance documents are not focused on any single sector and are not intended to imply regulatory requirements, but rather provide a systematic approach to reducing a broad spectrum of risks through effective assessment, planning, preparing, protection, response, and recovery. In addition to the NIPP, NPG, National Frameworks, and THIRA Guide described in Section 1 of this document, the following federal documents provide information directly or indirectly related to risk and security vulnerability assessment:

- **Comprehensive Preparedness Guide (CPG) 101, Developing and Maintaining Emergency Operations Plans** – Provides guidance for developing emergency operations plans, and promotes a common understanding of risk-informed planning and decision making to help planners examine a hazard or threat and produce integrated, coordinated, and synchronized plans.
- **CPG 502, Considerations for Fusion Center and Emergency Operations Center (EOC) Coordination** – Provides guidance for coordination between fusion centers and EOCs, and outlines their roles within the fusion. Fusion supports implementation of risk-based, information-driven prevention, response, and consequence management programs.
- **Homeland Security Exercise and Evaluation Program (HSEEP)** – Provides guiding principles for exercise programs as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. HSEEP supports consistency in developing, executing, and evaluating exercises that address priorities based on the NPG, threat and hazard identification/risk assessment processes, capability assessments, and results of previous exercises and real-world events.
- **National Incident Management System (NIMS)** – Provides guidance for all levels of government, nongovernmental organizations, and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents. NIMS provides a shared vocabulary, systems, and processes, and provides a common framework to integrate diverse capabilities during preparedness, response, and recovery operations.
- **Public Area Security National Framework (PASNF)** – Provides a strategy to share information, prevent attacks, and protect infrastructure from emerging threats to public spaces of transportation venues. One of the recommendations provided in the PASNF is to develop joint (public and private sector) risk frameworks and enhance joint vulnerability assessments.

Each of these documents provides information to be integrated into the risk and SVA methodology, either in the conduct of the assessment or in defining potential mitigation strategies.

B2 – Academic Research

Academic research documents reviewed for this project include:

- Estimating Terrorism Risk, Center for Terrorism Risk Management Policy, RAND Corporation
- Root Cause Analysis for Beginners, Quality Progress, American Society for Quality

- An Overview of Threat and Risk Assessment, SANS Institute
- Development of an Automated Security Risk Assessment Methodology Tool for Critical Infrastructures, Sandia National Laboratories

Each document is summarized below.

B2.1 Estimating Terrorism Risk

Estimating Terrorism Risk, released in 2005 by the RAND Corporation's Center for Terrorism Risk Management Policy, was one of the first documents to examine risk-based allocation of homeland security resources following the formation of DHS. The most useful data point in this document is the risk equation:

Risk = Threat x Vulnerability x Consequence (where Threat is probability)[16]

This equation was subsequently used in other SVA methodologies, and is recommended for use in support of airport-focused security and risk assessments.

B2.2 Root Cause Analysis for Beginners

In many cases, security and risk assessments are conducted for planning and/or design purposes using predefined hazard and threat scenarios. Assessment should also be considered after an incident has occurred as a method of identifying preventative strategies. Root Cause Analysis (RCA) is useful in post-event assessments to understand why an incident occurred. RCA typically involves four steps:[17]

1. Data collection
2. Causal factor charting
3. Root cause identification
4. Recommendation generation and implementation

Step 3 is the most compelling and differentiated from traditional security and risk assessment methodologies. Once all causal factors are identified, a Root Cause Map[18] is used to identify underlying reasons for each causal factor. The Root Cause Map uses a reasoning process to answer questions as to why a causal factor exists or occurred. For the purposes of post-event assessment, RCA provides benefits in identifying causal factors and potential methods of mitigating risks.

B2.3 An Overview of Threat and Risk Assessment

An Overview of Threat and Risk Assessment is a product of the SANS Institute and focuses on IT systems. Risk assessments focusing on IT systems generally require an entirely different team than is used in physical security and airport operational functions, and are an increasing concern as hacking incidents continue to increase in number and impact.

The document validates use of a risk register, and also provides a list of IT-security threats to consider in assessing risk as indicated in Table B-1.

[16] Willis, Henry H., et al. Estimating Terrorism Risk. Center for Terrorism Risk Management Policy. RAND Corporation, 2005, page 10.
[17] Rooney, James J. and Vanden Heuvel, Lee N. Root Cause Analysis for Beginners. Quality Progress, American Society for Quality, July 2004, pages 46–48.
[18] Rooney, James J. and Vanden Heuvel, Lee N. Root Cause Analysis for Beginners. Quality Progress, American Society for Quality, July 2004, page 49.

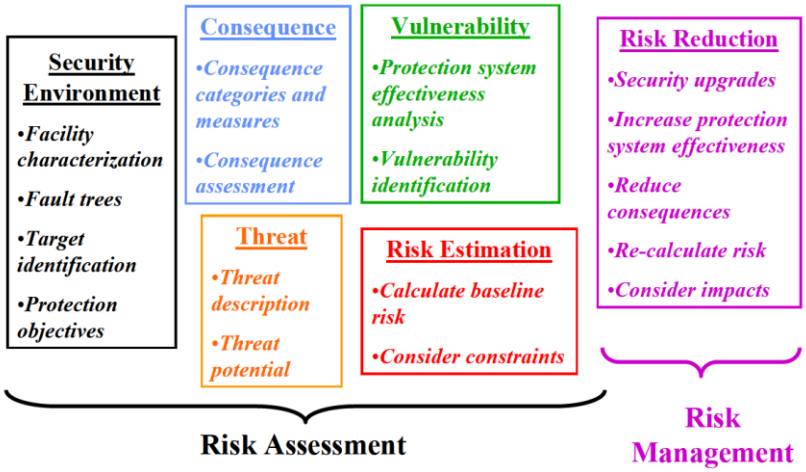
Table B-1. IT Security Reference Threats[19]

Human	Non-Human
Hackers	Floods
Theft (electronically and physically)	Lightning strikes
Non-technical staff (financial/accounting)	Plumbing
Accidental	Viruses
Inadequately trained IT staff	Fire
Backup operators	Electrical
Technicians, Electricians	Air (dust)
	Heat control

B2.4 Development of an Automated Security Risk Assessment Methodology Tool for Critical Infrastructures

Sandia National Laboratories has led development of Risk Assessment Methodologies (RAM) in the chemical, energy, and water sectors, as well as for community-level assessment. *Development of an Automated Security Risk Assessment Methodology Tool for Critical Infrastructures* describes an automated RAM prototype tool for critical infrastructures (RAM-CI™). This methodology provides a fault tree approach to determining the probability of a particular occurrence, and clearly identifies activities that must be performed in all risk assessment methodologies as indicated in Figure B-1.

Figure B-1. Activities Common to All Risk Assessment Methodologies



Source: Sandia National Laboratories

B3 – Security Trade Association: ASIS International

ASIS International has developed several relevant consensus guidelines as described below. Guidelines developed by ASIS International have been awarded designation under the Support Anti-Terrorism by Fostering Effective Technology Act of 2002 (SAFETY Act) by the DHS.[20] SAFETY Act designation ascribes a limit of liability against organizations who use the guidelines as a means to prevent or limit the scope of terrorist acts.

B3.1 Chief Security Officer Guideline

The Chief Security Officer (CSO) guideline establishes the CSO as the party responsible for gathering and assessing information regarding security threats and for assigning the resources and personnel to mitigate security risks. The guideline is also useful in establishing qualification guidelines for overall security and risk management.

[19] Bayne, James. An Overview of Threat and Risk Assessment. SANS Institute, 2002, page 6.
[20] Chief Security Officer Guideline, ASIS International, 2008, page 1.

B3.2 Security Management Standard: Physical Asset Protection

As it relates to physical asset protection, this Security Management Standard provides a similar model for risk assessment as previously described. It also provides guidelines to maintain a formal and documented risk treatment and countermeasure selection process including:[21]

1. Removing the risk source when possible
2. Avoiding the risk by temporarily halting activities that give rise to the risk
3. Removing or reducing the likelihood of a disruptive event and its consequences
4. Removing or mitigating harmful consequences
5. Sharing or transferring the risk with other parties (i.e., risk insurance)
6. Spreading the risk across assets and functions
7. Retaining risk by informed decision

B3.3 General Security Risk Assessment Guideline

The initial General Security Risk Assessment Guideline was developed after 9/11, and processes in this document are superseded by more recent releases. However, this document provides a list of information sources for determining loss risk events that may be helpful in data collection:[22]

- Local police crime statistics
- Uniform Crime Reports or comparable data
- Organization internal documents (e.g., security incident reports)
- Prior complaints from employees, customers, guests, visitors, etc.
- Prior civil claims for inadequate security
- Intelligence from local, state, or national law enforcement agencies about potential threats
- Industry-related information about trends
- General economic conditions of the area
- Presence of a crime magnet (e.g., proximity of a popular night club, property in disrepair)

B4 – Sector-Specific Guidance

As indicated previously, the NIPP identifies 16 critical infrastructure sectors, many of which have developed sector-specific risk and SVA methodologies. Risk management information regarding the aviation/airports, chemical, defense industrial base, energy, government facilities, IT, transportation, and water and wastewater sectors is provided below.

B4.1 Aviation/Airports

REGULATORY LANDSCAPE AND GUIDELINES

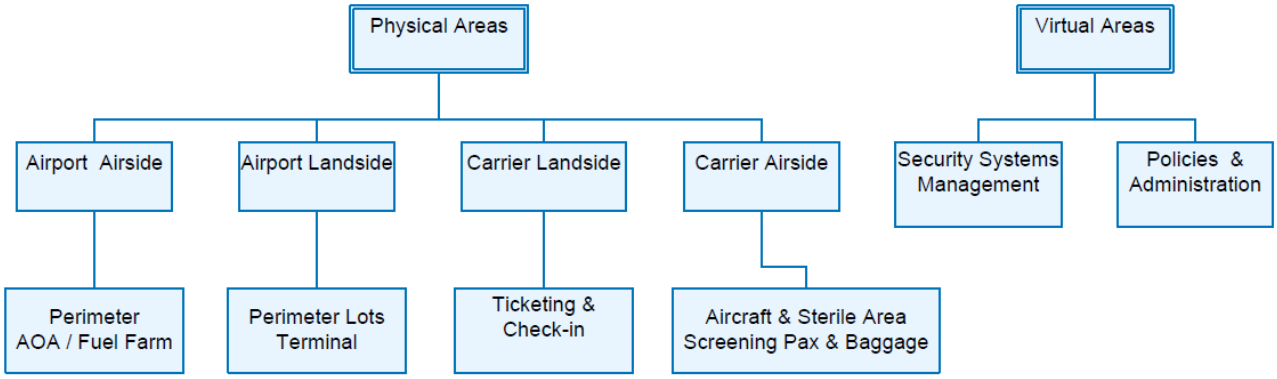
None of the applicable airport regulations (14 CFR § 139 – Certification of Airports, 49 CFR § 1540 – Civil Aviation Security: General Rules, and 49 CFR § 1542 – Airport Security) contain specific requirements to conduct a broad risk assessment. In addition to the federal guidance discussed previously, the following documents provide some guidance relative to risk and security vulnerability assessments:

- *Recommended Security Guidelines for Airport Planning, Design, and Construction*, U.S. Department of Homeland Security, Transportation Security Administration – Appendix A

[21] Security Management Standard: Physical Asset Protection, ASIS International, American National Standards Institute (ANSI)/ASIS Physical Asset Protection (PAP).1-2012, page 14.
[22] General Security Risk Assessment Guideline. ASIS International, 2003, page 7.

provides a general process for conducting vulnerability assessments and includes a model for assessing airport vulnerabilities as indicated in Figure B-2.

Figure B-2. Model for Assessing Airport Vulnerabilities[23]



- Information Circular IC 15-01E, Insider Threat. U.S. Department of Homeland Security, Transportation Security Administration, August 30, 2018 – This Information Circular recommends a vulnerability assessment and mitigation relative to a specific threat, and provides a checklist. No methodology is specified.

ACRP

ACRP Report 74: Application of Enterprise Risk Management (ERM) at Airports, defines ERM as "a structured, consistent, and continuous system that is applied across an entire organization to manage uncertainty."[24] As it pertains to risk assessment, Report 74 is consistent with other sources in its approach. In describing risk identification techniques, three unique terms are presented that have relevancy in developing an aviation-specific assessment methodology:

- **Business Impact Analysis** – Identifies resilience to various hazards and threats and the impact they may have on key airport processes.
- **Process Flow Analysis** – Identifies stepwise processes for operational functions and risks that may impede critical paths.
- **Scenario Analysis** – Identifies hazards and threats that would have significant impact, regardless of likelihood. Typically, worst-case and alternate-case scenarios are analyzed.

ACRP Report 112: Airport Terminal Incident Response Planning provides information on developing risk-based response plans specific to terminal operations. While the focus is on terminal operations, the information presented in Chapter 2, Methodology and Data Sources, includes two tables that characterize possible threats and hazards to airports. These tables, presented below, provide a value in identifying reference threats for an airport risk assessment methodology.

[23] Recommended Security Guidelines for Airport Planning, Design, and Construction, U.S. Department of Homeland Security, Transportation Security Administration, May 1, 2011, page 152.
[24] Report 74, Application of Enterprise Risk Management at Airports. Airport Cooperative Research Program, National Academy of Sciences, 2012, page 8.

Table B-2. Reference Threats and Hazards Sorted by Risk[25]

Threat/Hazard	Probability 3 = High 2 = Medium 1 = Low 0 = None	Consequences 4 = Very High 3 = High 2 = Medium 1 = Low 0 = None	Risk (Probability x Consequences)
Structural fire	2	4	8
Active shooter	2	3	6
Bomb threat	2	3	6
FAA navigation system failures	2	3	6
Irregular operations	2	3	6
Security breach	2	3	6
Security equipment malfunction	2	3	6
Traffic blockage (access roads)	2	3	6
Transit system failure (trams, people movers, access and functional needs transport, etc.)	2	3	6
Electrical outage/power failure	3	2	6
Suspicious package or bag	3	2	6
Biological agent	1	4	4
Bomb explosion	1	4	4
Hostage/barricade	1	4	4
Pandemic/quarantine	1	4	4
Structural failure of building	1	4	4
Aircraft diversion (non-signatory carrier)	2	2	4
Flight cancellations (local or distant)	2	2	4
Other criminal act requiring investigation, crime scene protection, and crowd control	2	2	4
Suspicious odor	2	2	4
Aircraft accident/crash	1	3	3
Aircraft hijacking	1	3	3
Chemical agent	1	3	3
Civil unrest/riot	1	3	3
Cyber-attack/disruption	1	3	3
Hazardous materials spill	1	3	3
Nonspecific threat of damage to people or terminal	1	3	3
Radioactive agent	1	3	3

[25] Report 112, Airport Terminal Incident Response Planning, Airport Cooperative Research Program. National Academy of Sciences, 2014, page 7.

Threat/Hazard	Probability 3 = High 2 = Medium 1 = Low 0 = None	Consequences 4 = Very High 3 = High 2 = Medium 1 = Low 0 = None	Risk (Probability x Consequences)
Usurpation/preemption of terminal facilities for regional disaster	1	3	3
Baggage system failure	3	1	3
False fire alarm	3	1	3
HVAC failure	1	2	2
Flood/sprinkler use in building	2	1	2
Picketing/protests/labor actions	1	1	1

Table B-3. Geographic-Specific Reference Hazards Sorted by Risk[26]

Threat/Hazard	Probability 3 = High 2 = Medium 1 = Low 0 = None	Consequences 4 = Very High 3 = High 2 = Medium 1 = Low 0 = None	Risk (Probability x Consequences)
Hurricane	3	3	9
Snowstorm	3	3	9
Earthquake	2	4	8
Tornado	2	4	8
Wildfire/smoke	2	3	6
Storm	3	2[1]	6
Dust storms/sandstorms	1	3	3
Tidal wave/tsunami	1	3	3
Wind-driven water	1	3	3
High water/flood	3	1	3
Volcanic eruption	1	2	2
Drought	0	0	0
Landslide/mudslide (may operate through blocking access roads)	0	0	0

[1]Consequences will be higher for storms (and most other geo-specific disasters) at airports that primarily serve regional jets and smaller airlines.

[26] Report 112, Airport Terminal Incident Response Planning, Airport Cooperative Research Program. National Academy of Sciences, 2014, page 8.

AIRPORTS COUNCIL INTERNATIONAL

The Landside Security Handbook, released by the Airports Council International in 2018, focuses specifically on threats that may impact landside operations, derived from actual events including:[27]

- **Fort Lauderdale-Hollywood International Airport** – Active shooter incident on January 6, 2017
- **Ataturk Airport, Istanbul, Turkey** – Active shooter and suicide bombings on June 28, 2016
- **Brussels Airport, Belgium** – Three coordinated suicide bombings at Brussels Airport and Maalbeek Metro Station on March 22, 2016
- **Domodedovo International Airport, Moscow, Russia** – Suicide bombing on January 24, 2011
- **Glasgow Airport, United Kingdom** – Terrorist ramming attack involving a sport-utility vehicle loaded with propane canisters on June 30, 2007

Further discussion of risk focusing on malevolent threats suggests a granular approach to describing possible threat scenarios as indicated below:[28]

Table B-4. Example Threat Scenario Characterization

Threat Scenario	Methodology (description of methods)	Responsibilities	Stakeholders
Person-borne improvised explosive device (PBIED) on body detonated at check-in area	Target/Asset: Check-in queue Adversary: Airport visitor Modus operandi: IED on the body, suicide attack	Law Enforcement Emergency Medical Services Intelligence Airport Authority	Airlines Concessions Ground Transportation
Description: A terrorist has gained access to the airport site, either on foot, via a taxi, car or public transport. The terrorist then detonates the PBIED within the airport site at the threshold or inside a critical asset. Risk to life.			

INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO)

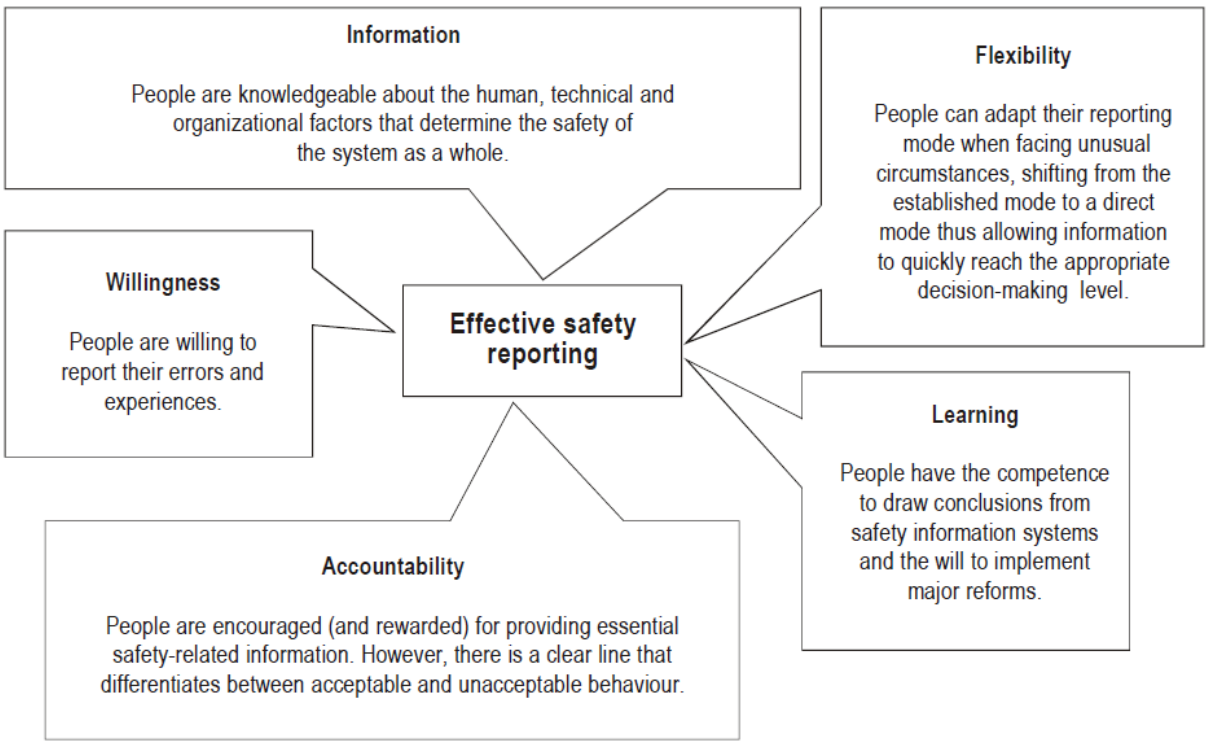
Three ICAO documents provide useful information in the formation of an airport-specific risk assessment methodology as describe below:

- **Aviation Security Manual** – This restricted[29] document advocates use of assessments to develop risk-informed security procedures, and provides a description of risk assessments. This document is consistent with other documents in its treatment of risk as a function of consequences and likelihood.
- **Risk Context Statement** – This document provides an annual assessment of global risks in the aviation sector. The identified threats and the global assessment of likelihood, consequence, vulnerability, and resulting risk is useful for airport management in defining reference threats during initial and annual risk and security vulnerability initiatives.
- **Aviation Safety Manual** – While focusing on safety rather than security, the risk assessment methodology within this document is much more defined than that within the Aviation Security Manual, and links assessment with the Safety Management System as a clear path to mitigating risk. Another useful component is a figure depicting effective safety reporting. Substituting

[27] Landside Security Handbook. Airports Council International, First Edition, 2018, pages 10–12.
[28] Landside Security Handbook. Airports Council International, First Edition, 2018, pages 13–14.
[29] Distribution of Doc 8973 is restricted to authorized entities and individuals. Access is subject to approval by the ICAO Aviation Security Policy Section and/or by the designated authority for aviation security in each respective Member State of the Organization.

"security" for "safety" in Figure B-3 may yield an effective model to enhance "See Something, Say Something" and other programs to support security awareness.

Figure B-3. Effective Safety Reporting[30]



PARAS

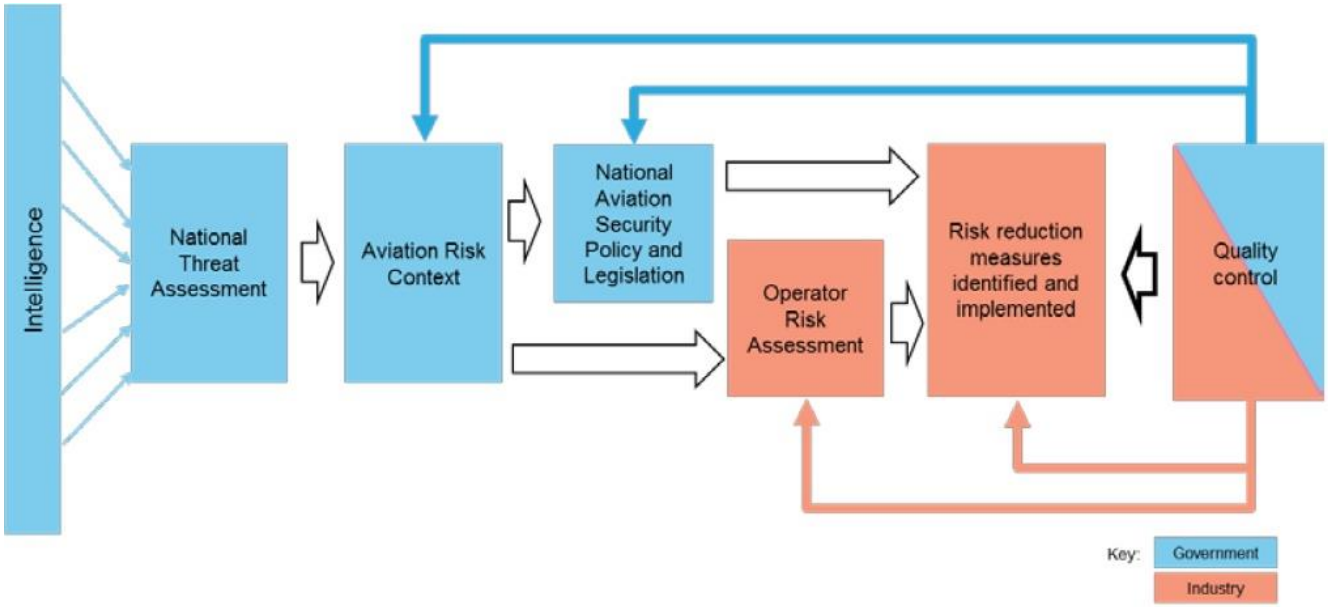
Of the currently available PARAS documents, those described below offer relevance in developing an airport-specific risk assessment methodology:

- **PARAS 0004: Recommended Security Guidelines for Airport Planning, Design, and Construction** – In Section 2, Initial Planning and Design Considerations, this document briefly describes vulnerability assessment as a means to support planning and facility protection. It also describes risk assessment in Section 3, Defining Operational Requirements. Appendix A, Section 2 provides some details to support conducting a risk assessment.
- **PARAS 0006: Employee Inspections Synthesis Report** – This document provides general acknowledgement of the need to consider insider threats in risk-based security management.
- **PARAS 0007: Quick Guide for Airport Cybersecurity** – This document provides a basis for identifying cybersecurity threats to airports, describes a risk assessment tool, and cybersecurity best practices to support mitigation of risk.
- **PARAS 0008: Findings and Practices in Sharing Sensitive Information** – This document indicates that threat, vulnerability, and risk assessment should be managed as SSI.
- **PARAS 0009: Guidance for Security Management Systems** – This document generally validates the importance of conducting threat and risk assessments as part of an effective Security Management System. It also links assessment to security management, and provides well-developed definitions regarding threat and risk components in the appendices. The processes discussed are consistent with other risk assessment methodologies.

[30] Aviation Safety Manual. International Civil Aviation Organization, Doc 9859 AN/474, Third Edition, 2013, page 2-17.

- **PARAS 0010: Guidance for Protecting Access to Vital Systems Impacting Airport Security** – This document generally advocates use of threat/vulnerability/risk assessments as a method of identifying vital airport systems and protecting access to them. The limited discussion of methodology is consistent with those previously described.
- **PARAS 0014: Blast Mitigation Strategies for Non-Secure Areas at Airports** – This document provides an observation of note that airports do not frequently convert risk assessments to specific security measures, in large part due to feasibility, impracticality, and cost. This observation indicates the need for guidance regarding a broad base of mitigation options to mitigate risk. In many circumstances, feasible lower- and medium-cost mitigation measures reduce risks substantially. Figure B-4, taken from the PARAS 0014 report, highlights an important distinction of responsibilities of the federal government (National Threat Assessment and National Aviation Security Policy and Legislation) and airport operators. The relevance is the importance of multilateral coordination between the airport operator and FAA and TSA officials in the planning, conduct, and post-implementation phase of a risk assessment.

Figure B-4. Risk Reduction Measures at the National and Operator Level[31]



Source: Arup USA, Inc.

B4.2 Chemical Sector

In the aftermath of 9/11, the chemical sector was one of the first to develop a sector-specific risk methodology. The universe of chemical facilities addressed is large and diverse and, due to regulations promulgated by the Environmental Protection Agency and the Occupational Safety and Health Administration before 9/11, this sector had prior risk assessment data to utilize from a security standpoint. Documents produced by various sector trade groups are summarized below:

AMERICAN CHEMISTRY COUNCIL (ACC)

The ACC, in conjunction with other trade associations, develops Site Security Guidelines and Transportation Security Guidelines specifically for the chemical sector. The general approach to risk

[31] Blass, Deborah. PARAS 0014: Blast Mitigation Strategies for Non-Secure Areas at Airports. Safe Skies, August 2018, page 32.

assessment is consistent with those previously described. Two criteria identified in the ACC document not previously discussed are:

- The importance of identifying a broad range of assets to consider during the assessment including:[32]
  - Automated processes (digital control systems, programmable logic controllers)
  - Backup power systems
  - Boilers
  - Control systems
  - Critical supplies
  - Electrical power lines
  - Hazardous materials
  - Natural gas lines
  - Rail lines and other transportation arteries
  - Storage tanks and pipelines
  - Telephone and data lines
  - Vehicles
  - Water supply, waste treatment facilities and equipment, and sewer lines
- The importance of management support in facilitating a secure environment as described in Table B-5.

Table B-5. Management Commitment Criteria[33]

No.	Criteria	Yes/No
1	Does top management visibly support security efforts?	
2	Have clear security policies been developed and promulgated?	
3	Are partnerships established with local, state, and federal law enforcement agencies, other public safety agencies, and surrounding communities?	
4	Are relationships and procedures with other management functions established to provide coordinated response to security incidents?	
5	Do employees understand how to report security incidents?	
6	Does a system exist for collecting and analyzing reports of security incidents?	
7	Are security awareness programs for employees and contractors in place?	
8	Do procedures exist for referring suspicious incidents and breaches of policy to management?	
9	Do policies exist for coordination with law enforcement?	
10	Are procedures for emergency response and crisis management in place?	

SYNTHETIC ORGANIC CHEMICAL MANUFACTURERS ASSOCIATION (SOCMA)

SOCMA coordinated with the ACC and produced a very similar document titled *Guidelines and Model for Analyzing the Vulnerability of Chemical Sites*. Noted differences include:

[32] Site Security Guidelines for the U.S. Chemical Industry. American Chemistry Council, et al, October 2001, page 5.
[33] Site Security Guidelines for the U.S. Chemical Industry. American Chemistry Council, et al, October 2001, page 28.

- As a component of threat likelihood, the SOCMA document describes attractiveness of the target as a contributing factor. SOCMA concluded that terrorist groups typically select targets based on factors such as visibility, national significance, symbolism, ease of planning, available resources, and status as critical infrastructure.[34]
- The SOCMA document also describes other factors that impact risk to a particular site, such as population density, proximity to surface water, distance to other critical infrastructure, government buildings, and military installations, and rail and maritime access.

AMERICAN PETROLEUM INSTITUTE (API)

- API developed the document *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*, which provides a methodology consistent with those previously described. The API document includes a comprehensive list of SVA supporting data requirements such as scaled facility drawings, aerial photography, and process flow diagrams.[35] The API document also discusses the importance of considering asset interdependencies throughout the SVA process.

B4.3 Defense Industrial Base Sector

While a great number of defense-related documents discuss risk assessment, the three documents described below provide the most directly applicable information to support development of an airport-specific risk and SVA methodology:

- **Emergency Response Planning for Military Water Systems, Technical Guide 297** – Developed by the U.S. Army Center for Health Promotion and Preventative Medicine, Water Supply Management Program, Technical Guide 297 advocates an approach similar to those previously described, and highlights the importance of linking SVAs to emergency and consequence management planning.
- **Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities (SCIF)** – Developed by the National Counterintelligence and Security Center, Office of the Director of National Intelligence, this document requires a risk assessment for any site proposed as a SCIF using similar terminology as those methodologies described previously. A unique concept relative to other documents is that of Security in Depth, which describes factors that enhance the probability of detection before actual penetration of the SCIF occurs.[36] This concept, while not entirely applicable, may have relevance to more critical airport assets.
- **Standard Practice for System Safety, Military Standard (MS) 882D** – Department of Defense MS 882D focuses on reducing safety risks to prevent mishaps, which are defined as "an unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment."[37] Most of the previously reviewed documents focus on assets rather than processes. MS 882D approaches risk assessment similarly to other methodologies, however the mishap severity categories (Table B-6) are applicable to assessing process risks.

[34] Guidelines and Model for Analyzing the Vulnerability of Chemical Sites. Synthetic Organic Chemical Manufacturers Association, August 16, 2002, page 6.
[35] Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries. American Petroleum Institute/National Petrochemical and Refiners Association, May 2003, page 45.
[36] Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.3. National Counterintelligence and Security Center, Office of the Director of National Intelligence, IC Tech Spec-for ICD/ICS 705, September 10, 2015, page 8.
[37] Standard Practice for System Safety, Department of Defense, Military Standard 882D, February 10, 2000, page 2.

Table B-6. Geographic-Specific Reference Hazards Sorted by Risk[38]

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation
Marginal	III	Could result in injury or occupational illness resulting in one or more lost workdays, loss exceeding $10K but less than $200K, or mitigatable environmental damage without violation of law or regulation where restoration activities can be accomplished
Negligible	IV	Could result in injury or illness not resulting in a lost workday, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation

B4.4 Energy Sector

The North American Electric Reliability Corporation completed a standard physical security for Critical Infrastructure Protection (CIP), CIP-014-2, on October 2, 2015. CIP-014-2 requires an initial risk assessment and subsequent risk assessments at least once every 30 or 60 calendar months, depending on the utility's status. While CIP-014-2 does not contain a complete risk assessment methodology, it suggests other standards, including ASIS International General Risk Assessment Guidelines, as useful resources. A unique quality of CIP-014-2 is the requirement to have an unaffiliated third party verify the risk assessment.[39]

B4.5 Government Sector

As defined in the NIPP and the Government Facilities Sector-Specific Plan, the government sector includes offices and housing for government employees, correctional facilities, embassies and consulates, education facilities, and courthouses, among others. Documents developed to support the government sector in risk reduction are described below.

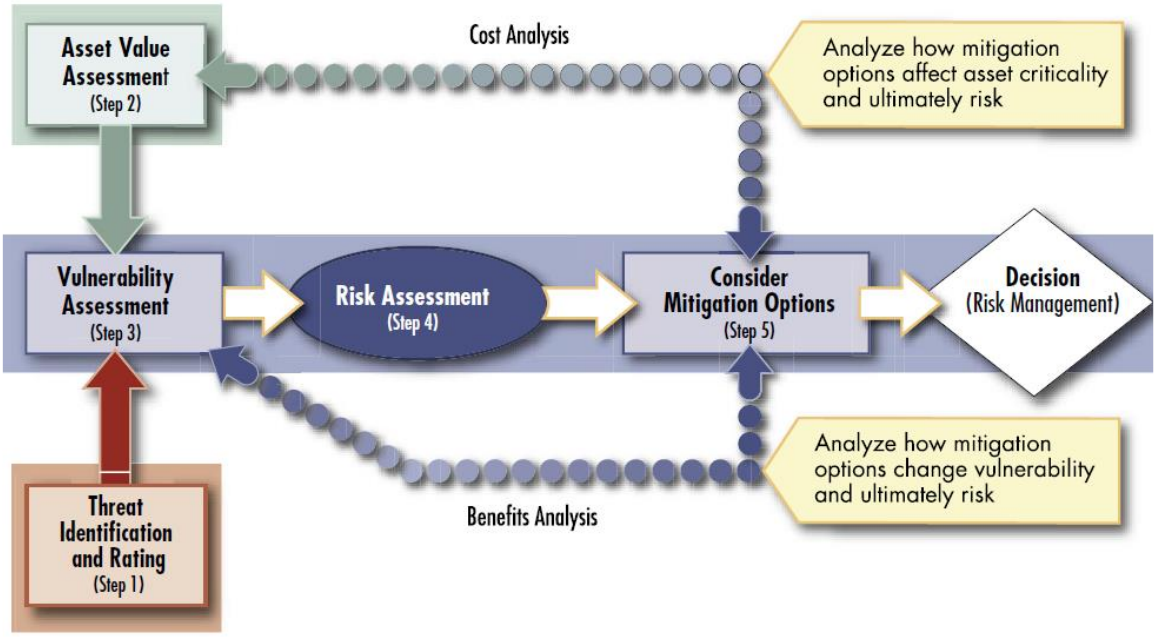
FEDERAL FACILITIES AND OTHER LITERATURE

Regarding assessment of general government facilities, two valuable sources of information are summarized below:

- Risk Assessment: A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings, Federal Emergency Management Agency (FEMA) 452 – Developed by FEMA in 2005, this document describes in great depth the process of conducting a risk assessment for malevolent threats. The process described is consistent with those previously described, however the depth of information, particularly regarding threat identification and rating, is much more advanced than other sources and includes detailed characterization of explosives and chemical, biological and radiological weapons. The process presented in the document is characterized in Figure B-5.

[38] Report 112, Airport Terminal Incident Response Planning, Airport Cooperative Research Program. National Academy of Sciences, 2014, page 8.
[39] CIP-014-2 – Physical Security, Critical Infrastructure Protection, North American Electric Reliability Corporation (NERC), October 2, 2015, page 3.

Figure B-5. Risk Reduction Measures at the National and Operator Level[40]



The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard – Released in August 2013, this document describes a process similar to those previously described, and introduces the concept of Facility Security Level (FSL) determination in the risk management process, as defined in Table B-7. This standard also introduces the concept of mixed-tenants/multi-tenant facilities as a consideration in assessing facility risk.

Table B-7. Interagency Security Committee Facility Security Level Determination Matrix[41]

Factor	Points				Score
	1	2	3	4	
Mission Criticality	Low	Medium	High	Very High	
Symbolism	Low	Medium	High	Very High	
Facility Population	< 100	101–250	251–750	> 750	
Facility Size	< 10,000 sq. ft.	10,001–100,000 sq. ft.	100,001–250,000 sq. ft.	> 250,000 sq. ft.	
Threat to Tenant Agencies	Low	Medium	High	Very High	
					Sum of above
Facility Security Level	I 5–7 Points	II 8–12 Points	III 13–17 Points	IV 18–20 Points	
Intangible Adjustment	Justification:				+ / - 1 FSL
					Final FSL

[40] Risk Assessment: A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings. Federal Emergency Management Agency, FEMA 452, January 2005, page iii.
[41] The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, 1st Edition, August 2013, page 6.

EDUCATION SUBSECTOR

In June 2013, two guides were released by the U.S. Department of Education, in cooperation with other federal agencies, to promote Emergency Operations Planning in higher education institutions and primary and secondary schools. Released largely due to an increase in gun violence, these documents advocate risk-based planning consistent with other guidance documents. A unique quality in these documents is the descriptions of various assessment types that may inform risk, as outlined in Table B-8.

Table B-8. Types of Assessments[42]

Assessment	Description	Purpose and Results
Site Assessment	Examines the safety, accessibility, and emergency preparedness of the buildings, facilities, and grounds. It includes, but is not limited to, a review of building access control measures, visibility around the exterior of the buildings, compliance with applicable architectural standards for individuals with disabilities and others with access and functional needs, structural integrity of the buildings, and emergency vehicle access.	• Increased understanding of the potential impact of threats and hazards on the buildings, facilities, and grounds. • Increased understanding of risk and vulnerabilities of the buildings, facilities, and grounds. • Knowledge of which facilities are physically accessible to individuals with disabilities and others with access and functional needs, and can be used in compliance with the law.
Climate Assessment	In a nurturing, inclusive environment, members of a community are more likely to succeed, feel safe, and report threats. If a student survey is used to assess culture and climate, student privacy must be protected. A range of personnel across the IHE can assist in the assessment of climate, including counselors and mental health staff.	• Knowledge of students' and staff's perceptions of their safety. • Knowledge of problem behaviors that need to be addressed to improve climate.
Threat Assessment	A campus threat assessment analyzes campus members' communications and behaviors to determine whether or not a member may pose a threat. These assessments must be based on fact; must comply with privacy, civil rights, and other applicable laws; and are often conducted by multi-disciplinary threat assessment teams. The assessment team is a separate entity from the planning team and meets on its own regular schedule.	• Students, staff, or other persons that may pose a threat are identified before a threat develops into an incident and are referred for services.
Capacity Assessment	A capacity assessment examines the capabilities of students, faculty, and staff, and the services and material resources of community partners to identify individuals with applicable training and skills (e.g., first aid certification, search and rescue training, counseling and mental health expertise). Equipment and supplies should also be inventoried, including an evaluation of supplies for individuals with disabilities and others with access and functional needs, such as evacuation chairs, the availability of sign language interpreters and technology used for effective communication, accessible transportation, and consumable medical supplies and durable medical equipment that may be necessary during a shelter-in-place or evacuation.	• An increased understanding of the resources available. • Information about staff capabilities will help planners assign roles and responsibilities in the plan.

[42] Guide for Developing High Quality Emergency Operations Plans for Institutions of High Educations. U.S. Department of Education, Office of Elementary and Secondary Education, Office of Safe and Healthy Students, June 2013, page 18.

B4.6 Information Technology Sector

The Risk Management Guide for IT Systems developed by the National Institute of Standards and Technology, provides a model for risk assessment of cybersecurity threats in the context of an overall risk management model. The basic steps for risk assessment relative to IT threats is similar to those previously described with two primary differences. First, the expertise necessary to conduct a cybersecurity threat assessment generally requires additional team members with significant experience in network and computer security. Second, in addition to identification and assessment of assets, threats, vulnerability, likelihood, and consequence as precursors to overall risk, this document suggests an additional step, control analysis. The goal of control analysis is to analyze controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood of a threat exercising a system vulnerability. The output of control analysis is a list of current or planned controls to mitigate vulnerabilities and reduce the impact of a given threat.[43]

B4.7 Transportation Systems Sector

References from the maritime, mass transit and passenger rail, and pipeline subsectors of the Transportation Systems Sector are summarized below.

MARITIME

Maritime facilities are regulated under 33 CFR § 105 and, while threat assessment is mentioned, no specific methodology is suggested or prescribed. In the United Nations document *Maritime Security: Elements of an Analytical Framework for Compliance Measurement and Risk Assessment*, three observations regarding risk assessment in maritime security are noted. First, regulatory risk assessment is typically reactive, and prompted and performed in response to an incident or threat of regulation. Second, not unlike the aviation sector, no established *industry framework* for security-risk assessment exists. Finally, very few countries have undertaken a structured and comprehensive regulatory assessment in relation to established international codes.[44] This document suggests a supply chain-oriented risk assessment framework based on three sources of risk:[45]

- Environmental: Uncertainties arising from external sources such as terrorist or environmental risks
- Organizational: Internal uncertainties arising within the supply chain such as strikes or production failures
- Network-related: Uncertainties arising from interactions between organizations in the supply chain

MASS TRANSIT AND PASSENGER RAIL

Documents addressing the mass transit and passenger rail subsector are summarized below:

- **Security and Emergency Preparedness Action Items for Transit Agencies, A Resource Document for Transit Agencies** – This document, developed by the U.S. Department of Transportation (DOT), Federal Transit Administration (FTA) and released in September 2014, recommends use of a risk assessment process to prioritize security investments. It also links risk

[43] The Risk Management Guide for Information Technology Systems developed by the National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-30, July 2002, page 20.
[44] Maritime Security: Elements of an Analytical Framework for Compliance Measurement and Risk Assessment, United Nations, UNCTAD/SDTE/TLB/2005/4, 2006, pages 8 – 9.
[45] Maritime Security: Elements of an Analytical Framework for Compliance Measurement and Risk Assessment, United Nations, UNCTAD/SDTE/TLB/2005/4, 2006, page 10.

assessment to emergency and security planning and conducting training and emergency exercises.

- **The Public Transportation System Security and Emergency Preparedness Planning Guide** – Released by the U.S. DOT, FTA in January 2003, this document follows the general theme of other risk assessment guidance. In addition to assessing security threats and risks, it emphasizes performing a capabilities assessment within transportation systems to identify gaps in capabilities to reduce threats, mitigate emerging issues, protect passengers, and support community response.[46]
- **Transit Security Design Considerations** – Released by the U.S. DOT, FTA in November 2004, this document contains information to support identification and implementation of mitigation strategies.

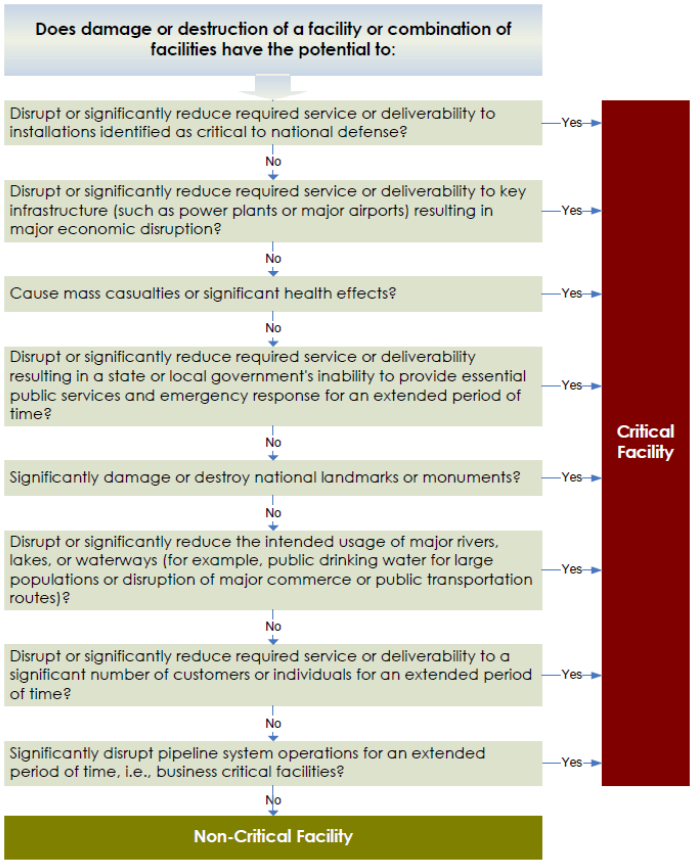
HIGHWAY INFRASTRUCTURE AND MOTOR CARRIER

A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection, released by the National Cooperative Highway Research Program provides direction on identifying critical ground transportation assets to support assessment of landside operations.

PIPELINE

Pipeline Security Guidelines, released by the DHS, TSA in March 2018, provides recommendations for security and risk assessment consistent with other documents. A unique aspect of this document that may be adaptable for airports is the treatment of criticality of facilities as provided in Figure B6.[47]

Figure B-6. Criticality Determination Pathway



B4.8 Water and Wastewater Systems Sector

The Risk Analysis and Management for Critical Asset Protection Standard (also referred to as J100) was developed over several iterations since 2004, and was referred to in various drafts of the NIPP including the final 2006 version. The American National Standards Institute (ANSI), American Society of Mechanical Engineers (ASME)-Innovative Technologies Institute, LLC, and the American Water Works Association (AWWA) formally adopted it as the J100-10 standard on July 1, 2010. From its roots in the NIPP, the J100 standard was initially developed for the water sector but is adaptable to various critical infrastructures.

[46] The Public Transportation System Security and Emergency Preparedness Planning Guide, U.S. Department of Transportation, Federal Transit Administration, DOT-FTA-MA-26-5019-03-01/ DOT-VNTSC-FTA-03-01, Final Report, January 2003, page 47.
[47] Pipeline Security Guidelines. U.S. DHS, TSA, March 2018, page 9.

The J100 standard includes seven steps to fully assess a broad range of risks including natural hazards, malevolent threats, and dependencies:[48]

1. Asset Characterization:
    a. Identify the mission or critical functions to determine which assets perform or support the mission or critical functions
    b. Identify a list of potentially critical assets
    c. Identify critical internal and external supporting infrastructures
    d. Identify and document existing protective countermeasures and mitigation measures/features
    e. Estimate the worst reasonable consequences resulting from the destruction or loss of each asset without regard to the threat
    f. Prioritize critical assets using the estimated consequences
2. Threat Characterization:
    a. Identify general and specific threat scenarios (based on reference threats in J100) to serve as reference threats for the remainder of the process
    b. Malevolent threats include various modes of attack (e.g., air, land, and water), various magnitudes of attack elements, and attacks by both insiders (e.g., current or past employees, suppliers with access to facilities) and outsiders (e.g., adversaries, criminals, vandals)
    c. Natural hazards include hurricanes, floods, tornadoes, earthquakes, and wildfires
    d. Dependency hazards shall include interruptions of utilities, suppliers, employees, customers, and transportation, and proximity to dangerous neighboring facilities
3. Consequence Analysis: Identify the worst reasonable consequence for specific threats and include common quantitative metrics:
    a. Number of fatalities
    b. Number of serious injuries
    c. Financial loss to the owners of the facility
    d. Economic loss to the community (i.e., standard metropolitan area) in which it operates
4. Vulnerability Analysis: Analyze the ability of each critical asset and its protective systems to withstand each specified threat via processes provided in the J100 standard
5. Threat Analysis: Analyze the probability of hazards and threats occurring based on historical record or proxy measures
6. Risk and Resilience Analysis: Calculate risk and resilience measures based on previous data, and prioritize risks
7. Risk and Resilience Management: Develop countermeasures and mitigation options, estimate investment and operating costs, and develop an implementation plan

Reference threats and processes for each step are provided in the J100 standard. Augmented with findings in other documents, J100 provides a substantial baseline from which an effective airport-specific risk and SVA methodology can be developed.

[48] Risk Analysis and Management for Critical Asset Protection, American National Standards Institute (ANSI)/American Society of Mechanical Engineers (ASME)-Innovative Technologies Institute, LLC/American Water Works Association (AWWA), J100-10, First Edition, July 1, 2010, pages 6–15.

Stakeholder Survey Results

Ross and Baruzzini conducted an online survey as well as several phone interviews with airport representatives to gain insight into the current industry understanding of SVAs, the conduct of SVAs or similar assessments (such as a TSA Joint Vulnerability Assessment [JVA]), and the user's expectations for a practical guide and useful tools. Survey respondents, 20 in total, were from a variety of small (5), medium (5), and large (10) hub airports serving both large metropolitan areas and smaller, rural communities.

Survey questions were structured to gather information from each airport regarding their specific experience in the conduct or receipt of an SVAs or similar assessment.

TREND DATA

1. All (100%) of the medium and large hub airports surveyed received a JVA in the last 5 years
    - The level to which TSA involved the airport operator in JVAs varied greatly from 'none at all' to 'a great deal.'
    - Of airports that were involved in the JVA 'a great deal,' 100% reported that the JVA process and findings provided value to the airport and led to security improvements (e.g., capital improvements, update to procedures, upgrades to equipment) as a result of the JVA.
    - Of those airports that reported little to no involvement in the JVA process, only 40% reported that the JVA provided value to the airport and led to security improvements as a result of the JVA.

Findings: Success and value of a JVA to an airport is directly related to the level of involvement of the airport operator in the assessment. Those airports with a positive working relationship with their FSD and local TSA tended to have more a positive experience and output from the JVA.

Supporting Quotes:

- "You have to be VERY vocal with local TSA that you expect to partner with them on the JVA. If you do not remind them, you want to be a part of the process they will do it without you."
- "Great partnership, good explanation of the goals of protecting the nationwide single 'sterile' area that is connected via airports, very clear upfront that the assessment is not punitive and will not lead to civil sanctions or regulatory investigations."
- "Recommend they work more closely with Airport personnel or bring in other Airport Public Safety team members who have experience and knowledge of all the Airport Operations."
- "Meetings were held both prior and after the JVA was conducted. My impression is that the team conducting the assessment was not provided sufficient time to do a thorough job."

2. Of the 20 total respondents, 65%—(9) large, (3) medium, and (1) small hub airports—have conducted an internal or third-party (contractor) SVA in the last five years.
    - Six of 13 airports conducted an internal assessment while the remaining seven airports hired a consultant to conduct the assessment.
    - 69% utilized a locally developed questionnaire and methodology; two airports utilized PARAS guidance and guidance from Argonne National Laboratories to develop their methodology
    - 31% did not know what methodology was used
    - Reasons cited for conducting the assessment:

Accident, incident, threats	33.33%	4
Terminal construction/improvements	25.00%	3
Justify new equipment	16.67%	2
Organizational changes or organizational direction	16.67%	2
Request or directive from regulatory agency	16.67%	2
Safety/security reports – i.e. increase in violations	16.67%	2
Grant monies desired	8.33%	1
Justify increase in personnel	8.33%	1
Special event	8.33%	1

- "Other" reasons cited:
  - New hotel and transit center as well as Main Terminal Renovation – 1
  - Internal Threat Mitigation Pilot Program – 1
  - Domestic and International Public Area threats that led to an airport-wide assessment – 1
  - Continued updating of our Security Master Plan – 1

Findings: There is a clear need for an airport-specific methodology for the conduct of SVAs as only 2 airports were able to reference any guidance at all. The primary reasons cited for the initiation of the SVA were as the result of an accident, incident, or threat; and terminal construction/improvements.

3. Airport department/stakeholders involved in gathering information and conduct of the assessment. This information can be used to populate the planning checklist.

Airport Security and Badging	100.00%	12
Airport Law Enforcement	100.00%	12
Airport Operations (Landside, Airside, Terminal)	91.67%	11
Airport Maintenance	75.00%	9
Transportation Security Administration (TSA)	75.00%	9
Airport Emergency Management	66.67%	8
Customs and Border Protection (CBP)	58.33%	7
Federal Bureau of Investigation (FBI) Airport Liaison (if applicable)	58.33%	7
Airport Dispatch/Communication Center and/or Operations Center	50.00%	6
Security services/ security contractor	50.00%	6
Fuel Provider	41.67%	5
Airport Safety and/or Risk	33.33%	4
Airline Station Managers	33.33%	4
Airport Rescue and Firefighting (ARFF)	25.00%	3
Air Cargo Operators	16.67%	2
Terminal concessionaires	16.67%	2
Baggage Handling Company or Organizational Representative	8.33%	1
Parking, Rental Car and Ground Transportation providers	8.33%	1
Skycap and janitorial service companies	8.33%	1
Other (please specify) Responses	8.33%	1

Other: IT department

Stakeholders deemed most valuable in providing relevant information for the assessment. Stakeholders are arranged in descending order of number of respondents that listed the stakeholder. This information can be used to populate the planning checklist.

1. Local and Airport Law Enforcement
2. Airport/Aviation Security Department
3. Airport Operations
4. TSA
5. Facilities/Maintenance
6. Engineering
7. IT
8. Fuel providers
9. Dockmaster, Fuel Company

4. Tools and practices used to inform participants and conduct the assessment.

Preliminary meetings with senior leadership	83.33%	10
Small group discussions	83.33%	10
Airport diagrams (as applicable to areas being assessed)	75.00%	9
Facilitated one-on-one interviews with participants	58.33%	7
Preliminary list of threats, risks, scenarios	41.67%	5
Checklist or template	33.33%	4
Manual worksheet or survey distributed to participants	16.67%	2
PowerPoint briefings for participants	16.67%	2
Training for leadership and/or participants on the SVA/TVA – why, how, goals, etc.	8.33%	1
Electronic worksheet or survey distributed to participants	0.00%	0
Handouts for participants	0.00%	0

Tools and practices deemed most useful:

- Spreadsheets detailing and identifying concerns and options or considerations, as well as response and current status
- Checklists, interviews
- Collecting priority needs from stakeholders via small group discussions and validating with senior leadership
- The briefings and small group discussions provided different vantage points of some of the same issues
- Group discussions were the most valuable; more heads leads to more ideas/suggestions.
- Group discussions were the most useful; Checklists were least since they did not address risk mitigation considerations
- Discussions and tours
- Facilitated interviews were the most effective; Written surveys/questionnaires were the least effective
- Senior level briefing

Findings: Airport utilized a variety of tools to conduct the SVA, however, group discussions and facilitated interviews were cited as most valuable by respondents.

5. Threat Scenarios utilized for the assessment.

Improvised explosive device (IED) - placed in airport or on aircraft		75.00%	9
Vehicle borne improvised explosive device (VBIED)		75.00%	9
Improvised explosive device (IED) – on person, suicide bomber		66.67%	8
Insider threat		66.67%	8
Active shooter		58.33%	7
Common crime (fraud, theft, drug smuggling, etc.)		41.67%	5
Sabotage – equipment		33.33%	4
Chemical or biological attack		25.00%	3
Cyber attack		16.67%	2
MANPAD attack		16.67%	2
Other (please specify)	Responses	16.67%	2
Hijack		8.33%	1
Attack using remotely piloted aircraft		0.00%	0

Other: Breach of perimeter

6. Challenges in conducting the assessment.

Conflicting opinions about what constitutes a threat to the airport and/or what threat to focus on		41.67%	5
Difficulty in scheduling meetings and interviews		33.33%	4
Financial/budget constraints		25.00%	3
Time required to set up and prepare for the SVA/TVA		25.00%	3
Time required to complete the SVA/TVA		16.67%	2
No challenges		16.67%	2
Difficulty in finding participants best suited to provide relevant information/data		8.33%	1
Difficulty in finding a facilitator		8.33%	1
Lack or support/buy-in from senior leadership and management		8.33%	1
Conflicting opinions about what constitutes critical airport assets/targets		8.33%	1
Other (please specify)	Responses	8.33%	1

Other: Ongoing time and resources for continuous evaluation

Findings: The primary challenge experienced by airports is the conflicting opinions about what constitutes a threat and which threats to focus on. Difficulty in setting up interviews, and financial and time constraints were also cited most as being a challenge. This supports our recommendations for involving local law enforcement and the FBI in developing a threat profile for the airport and in the methodology provided for choosing the threats

7. Additional insights, all responses are quoted from survey.
   - "Although we do periodic assessments, we also struggle with lack of time, funds, and overall resources to conduct and/or take action."
   - "The TSA JVA and the contractor assessments have both proven very helpful when planning future security projects."
   - "I strongly suggest any Risk Assessment or similar document be made as a living document that is updated frequently as airport layouts and operations evolve. Hundred-page shelf queens need not apply."
   - "Ongoing assessments and work to improve security help as much as full-blown assessment, however, outside opinions are always helpful."

- "Help provide long term strategies to keep the discussions/assessments going as threats evolve and mitigations are implemented."
- "Guidance in this area would be a great help to small airports"
- "Can help focus priorities on activities/projects that have a high security benefit and low (or lower) cost. Aviation Security Department can incorporate its priorities/projects into the study."

APPENDIX C: AIRPORT SECURITY VULNERABILITY ASSESSMENT CHECKLISTS

C1 – Project Charter

The Project Charter provided in Table C-1 establishes the parameters for conducting an Airport SVA including scope, schedule, budget (if applicable), and assigned team members/ participants. It is designed to facilitate successful completion of the SVA based on the established scope, schedule, and budget.

Table C-1. Project Charter Example

Project Title: Airport Security Vulnerability Assessment (SVA) Date of Charter: <Enter Date>

A. Scope		
1. Threat Focus	<Limited vs. Comprehensive and Quantitative vs. Qualitative>	
2. Asset/Function Focus	<Airside, Landside, Terminal, Cyber, Comprehensive>	
3. Desired Goal	The SVA is being initiated to support the airport in improving <enter goal>.	
B. Assigned Team		
Position	Name	Contact Information
1. SVA Project Manager	<Enter name and title>	
2. Team Members/Functions	<Enter name, title, and function>	
	<Enter name, title, and function>	
	<Enter name, title, and function>	
	<Enter name, title, and function>	
	<Enter name, title, and function>	
	<Enter name, title, and function>	
	<Enter name, title, and function>	
	<Enter name, title, and function>	
	<Enter name, title, and function>	
	<Enter name, title, and function>	
3. Stakeholder Participants (Airlines, concessions, regulatory agencies, etc.)	<Enter name, title, and organization>	
	<Enter name, title, and organization>	
	<Enter name, title, and organization>	
	<Enter name, title, and organization>	
	<Enter name, title, and organization>	
	<Enter name, title, and organization>	
	<Enter name, title, and organization>	
	<Enter name, title, and organization>	
	<Enter name, title, and organization>	
	<Enter name, title, and organization>	
C. Schedule		
1. Start Date	<Enter authorized starting date>	
2. Milestones	<Describe milestone and desired date>	
	<Describe milestone and desired date>	
	<Describe milestone and desired date>	
	<Describe milestone and desired date>	
	<Describe milestone and desired date>	

3.	Completion Date	<Enter desired completion date>
D.	**Budget/Resources**	
1.	Budget	<Enter budget, if applicable>
2.	Resources Available	<Identify any resources available such as subject matter experts, technology, or external contract support.>
E.	**Additional Instructions**	

<Provide any additional instructions regarding scope, purpose, regulatory concerns, etc. that will assist in completing the SVA effectively and efficiently>

Authorized by: _____
(signature)

Title _____ Date _____

C2 – Asset Characterization Tools

Asset Characterization Tools assist the SVA project team in identifying critical assets to be considered during SVAs. A critical asset is one that, if rendered inoperable, degrades the airport's ability to carry out its mission, or elicits other detrimental impacts relating to health and safety of airport patrons and employees, operational or financial losses, or political consequences. Single points of failure (i.e., assets for which there are no backups or workarounds) that impact the mission are of particular importance during the SVA process.

Table C-2 serves as a starting point and identifies potential critical reference assets based on these categories: A) Airside Operations and Secured Areas, B) Terminal Operations (Public), C) Landside Operations, and D) Infrastructure. Complete each column to create a list of assets to consider in the SVA, and to identify conditions and mitigation factors in place that may reduce risk relative to the asset. Complete Table C-3, Critical Asset Characterization Checklist, for each asset identified in Table C-2 to fully characterize each asset. Tables C-2 and C-3 correspond to Tabs 1 and 2 in the SVA Tools.

Table C-2. Critical Asset Identification Checklist

Asset	**Critical to Mission?** (yes/no)	**Backup?** (yes/no)	**Work-Around?** (yes/no)	**Single Point of Failure** (yes/no)
A. Airside Operations and Secured Areas				
1. Access Control System				
2. Aircraft Hydrant Fueling System				
3. Aircraft Rescue & Firefighting Facilities/Resources				
4. Airfield Navigation Systems				
5. Airport Authority Operations & Maintenance Facilities				
6. Cargo Facilities				
7. Catering Facilities				
8. Checked Baggage Screening/Operations/Makeup Areas				
9. Concession Storage Areas				
10. Deicing Systems				
11. Federal Inspection Stations				
12. Fuel Farm				
13. General/Business Aviation Areas				
14. Ground Run-up Enclosure				
15. Jet-Bridge Access				
16. Movement Areas (runways and taxiways)				
17. Non-movement Area Vehicle Access Points				
18. Perimeter Fencing				
19. Perimeter Intrusion Detection System				
20. Vehicle Gates				
21. Other:				
22. Other:				
B. Terminal Operations (Public)				

	Asset	Critical to Mission? (yes/no)	Backup? (yes/no)	Work-Around? (yes/no)	Single Point of Failure (yes/no)
1.	Baggage Claim				
2.	Concessions				
3.	Security Screening Checkpoints				
4.	Ticket Counters/Automated Check-In Areas				
5.	Other:				
6.	Other:				
C.	**Landside Operations**				
1.	General Traffic/Curbside Management Operations				
2.	Ground Transportation Operations				
3.	Parking Operations				
4.	Rental Car Operations				
5.	Other:				
6.	Other:				
D.	**Infrastructure**				
1.	Airport Authority Administrative Offices				
2.	Airport Authority Ground Vehicle Fueling Systems				
3.	Audio Communication Systems				
4.	Cellular Communication Systems				
5.	Common Use Information Technology/Networks				
6.	Dispatch/Communications Centers				
7.	Electrical Power Services				
8.	First Responder Communication Systems				
9.	Heating, Ventilation, Air Conditioning (HVAC) Systems				
10.	Law Enforcement Facilities and Resources				
11.	Mechanical, Electrical, Plumbing (MEP)				
12.	Natural Gas Services				
13.	Potable Water Services				
14.	Radio Communications Systems				
15.	Sewer Systems				
16.	Stormwater Systems				
17.	Vendor Deliveries				
18.	Vertical Circulation Systems				
19.	Video Communication Systems				
20.	Video Surveillance Systems				
21.	Waste Management Systems				
22.	Other:				
23.	Other:				
Notes					

The Checklist provided in Table C-3 is intended to be used to characterize each critical asset identified in Table C-1. Information gathered should inform: 1) Consequences of threats applied to assets, 2) Vulnerability of assets, 3) Measures to mitigate risk posed by specific threats, and 4) Costs associated with loss of the asset and workarounds.

Table C-3. Critical Asset Characterization Checklist

	Criteria	Description
1.	Category	<Airside Operations and Secured Areas; Terminal Operations; Landside Operations; or Infrastructure Systems>
2.	Asset	<List Asset>
3.	Asset Function	<Briefly describe primary asset function>
4.	Describe Asset Criticality	If this asset is out of service, what are the potential ramifications:
		Degradation of Service?
		Airport Full/Partial Closure?
		Injury to Patrons and Employees?
		Fatalities?
		Economic Impacts?
		Other?
5.	Down-Stream Dependencies	List other critical assets that depend on this asset to operate properly:
6.	Up-Stream Dependencies	List other critical assets upon which this asset is dependent to operate (e.g., power, fuels, water, etc.):
7.	Describe existing mitigation measures or security hardening in place to protect this asset.	
8.	Describe any existing backups for this asset (e.g., redundant systems, backup generators, etc.).	
9.	Describe any workarounds that could be implemented if this asset is out of service. Include cost of work-around if possible.	
10.	Estimate of replacement value for this asset.	
11.	Asset deemed critical to include in the SVA?	Yes ☐ No ☐

Asset Characterization Notes

<Provide any additional relevant details regarding the asset and its characteristics.>

Completed by: _____
(signature)

Title _____ Date _____

C3 – Airport Threat Characterization Tools

A list of reference threats and their definitions are provided in Table C-4. These are referred to in the blank Airport Asset-Threat Characterization Tool in Table C-5 to support evaluation of asset-threat combinations.

Table C-4. Threat Type Definitions

Threat Type	Definition
Armed Attack	Attack by one or more persons using firearms or other weapons
Arson	Deliberately setting fire to property
Assault	Physical or verbal attack on one or more persons involving patrons and/or employees
Attack: Explosives <=5 kg TNT Equivalent	– An attack using an explosive or IED such as a package or pipe bomb, mail/courier delivered package, or possibly drone-dropped
Attack: Explosives <=15 kg TNT Equivalent	An attack using an explosive or IED such as a backpack or luggage bomb
Attack: Explosives <=500 kg TNT Equivalent, Small VBIED	An attack using a small vehicle-borne IED (VBIED) to deliver to target, such as a passenger car
Attack: Explosives >=500 kg TNT Equivalent, Large VBIED	An attack using a large VBIED to deliver to target, such as a van or truck
Attack: Release of Infectious Agents	An attack releasing biological, chemical, or radiological agents in public areas
Civil Disorder/Protest	Disturbance of the public peace by multiple persons, generally in public areas such as roadways or terminals, which may impact operations
Sabotage	Deliberately destroying damaging, or obstructing property in such a way as to render it inoperable, generally for economic or political reasons
Theft	To steal property within the airport, generally for personal gain
Trespassing	To enter secure areas without permission or consent
Vandalism	Deliberate malicious act to damage or destroy property
Vehicle as a Weapon	An attack (not involving explosives) using a vehicle to inflict damage on people, property, or operations

The potential impact of a threat on a specific asset should be evaluated using a low, medium, or high designation, as defined below:

- Low (L) – A critical asset sustains little or no damage if subjected to the threat (no loss of service)
- Medium (M) – A critical asset sustains low to medium damage if subjected to the threat (loss of service is < 1 day and workarounds or backups allow continued operation)
- High (H) – A critical asset sustains medium to high damage or destruction if subjected to the threat (loss of service is >1 day and critical operations are out of services)

Critical assets determined to be unaffected by a particular threat should be designated ‘not applicable’ (NA). At the discretion of SVA project team, asset-threat combinations with estimated potential impacts of NA or low may be eliminated from further steps.

Alternatively, the SVA team may elect to use the completed tool provided in Tab 3 of the SVA Tools.

Instructions: The SVA team should use this table to designate asset-threat combinations as low, medium, high, or not applicable for each asset threat combination for both outsiders and insiders. Generally, insider threats are more likely in airside operations and Secured Areas as opposed to outsider threats. The SVA team should review each combination and evaluate based on local conditions and consensus among team members. Asset-threat combinations designated as medium or high are assessed in subsequent steps of the SVA.

Table C-5. Airport Asset-Threat Characterization Tool

Asset	Threat																									
	Armed Attack		Arson		Assault		Attack: Explosives <=5kg TNT Equivalent		Attack: Explosives <=15kg TNT Equivalent		Attack: Explosives >=500Kg TNT Equivalent – Large VBIED		Attack: Explosives <=500Kg TNT Equivalent – Small VBIED		Attack: Release of Infectious Agents		Civil Disorder		Sabotage		Theft		Trespassing		Vandalism		Vehicle as a Weapon	
Outside (O)/Insider (I)	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**
A. Airside Operations and Secured Areas																												
1. Access Control System																												
2. Aircraft Hydrant Fueling System																												
3. Aircraft Rescue and Firefighting Facilities and Resources																												
4. Airfield Navigation Systems																												
5. Airport Authority Operations & Maintenance Facilities																												
6. Cargo Facilities																												
7. Catering Facilities																												
8. Checked Baggage Screening/Operations/Makeup Areas																												
9. Concession Storage Areas																												
10. Deicing Systems																												
11. Federal Inspection Stations																												
12. Fuel Farm																												
13. General/Business Aviation Areas																												
14. Ground Run-up Enclosure																												
15. Jet-bridge Access																												
16. Movement Areas (runways and taxiways)																												
17. Non-movement Area Vehicle Access Points																												
18. Perimeter Fencing																												
19. Perimeter Intrusion Detection System																												
20. Vehicle Gates																												
21. Other:																												
22. Other:																												
23. Other:																												
24. Other:																												
B. Terminal Operations (Public)																												
1. Baggage Claim																												
2. Concessions																												
3. Security Screening Checkpoints																												
4. Ticket Counters/Automated Check-In Areas																												
5. Other:																												
6. Other:																												
7. Other:																												
8. Other:																												
C. Landside Operations																												

Asset	Threat																											
	Armed Attack		Arson		Assault		Attack: Explosives <=5kg TNT Equivalent		Attack: Explosives <=15kg TNT Equivalent		Attack: Explosives >=500Kg TNT Equivalent – Large VBIED		Attack: Explosives <=500Kg TNT Equivalent – Small VBIED		Attack: Release of Infectious Agents		Civil Disorder		Sabotage		Theft		Trespassing		Vandalism		Vehicle as a Weapon	
Outside (O)/Insider (I)	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**	**O**	**I**
1. General Traffic/Curbside Management Operations																												
2. Ground Transportation Operations																												
3. Parking Operations																												
4. Rental Car Operations																												
5. Other:																												
6. Other:																												
7. Other:																												
8. Other:																												
D. Infrastructure																												
1. Airport Authority Administrative Offices																												
2. Airport Authority Ground Vehicle Fueling Systems																												
3. Audio Communication Systems																												
4. Cellular Communication Systems																												
5. Common Use Information Technology/Networks																												
6. Dispatch/Communications Centers																												
7. Electrical Power Services																												
8. First Responder Communication Systems																												
9. Heating, Ventilation, Air Conditioning (HVAC) Systems																												
10. Law Enforcement Facilities and Resources																												
11. Mechanical, Electrical, Plumbing (MEP)																												
12. Natural Gas Services																												
13. Potable Water Services																												
14. Radio Communications Systems																												
15. Sewer Systems																												
16. Stormater Systems																												
17. Vendor Deliveries																												
18. Vertical Circulation Systems																												
19. Video Communication Systems																												
20. Video Surveillance Systems																												
21. Waste Management Systems																												
22. Other:																												
23. Other:																												
24. Other:																												
25. Other:																												

An example of a complete list of reference asset-threat combinations for airports is provided in Table C-6. Since conditions may vary among different airports, asset-threat combinations should be reviewed and assessed by the SVA project team for their specific airport and conditions.

Table C-6. Reference Asset-Threat Combinations for Airports

	Asset-Threat Combinations (Outsider/Insider)
A.	**Airside Operations and Secured Areas**
1	Access Control System
1.1	Sabotage (O/I)
1.2	Theft (O/I)
2	Aircraft Hydrant Fueling System
2.1	Armed Attack (I)
2.2	Arson (O/I)
2.3	Assault (I)
2.4	Attack: Explosives <=5kg TNT Equivalent (O/I)
2.5	Attack: Explosives <=15kg TNT Equivalent (O/I)
2.6	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
2.7	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
2.8	Sabotage (I)
2.9	Vandalism (I)
2.10	Vehicle as a Weapon (I)
3	Aircraft Rescue and Firefighting Facilities and Resources
3.1	Armed Attack (O/I)
3.2	Assault (I)
3.3	Attack: Explosives <=5kg TNT Equivalent (O/I)
3.4	Attack: Explosives <=15kg TNT Equivalent (O/I)
3.5	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
3.6	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
3.7	Attack: Release of Infectious Agents (I)
3.8	Sabotage (O/I)
3.9	Theft (O/I)
3.10	Vandalism (O/I)
3.11	Vehicle as a Weapon (O/I)
4	Airfield Navigation Systems
4.1	Sabotage (O/I)
4.2	Vandalism (I)
5	Airport Authority Operations & Maintenance Facilities
5.1	Armed Attack (I)
5.2	Arson (I)
5.3	Assault (I)
5.4	Attack: Explosives <=5kg TNT Equivalent (I)
5.5	Attack: Explosives <=15kg TNT Equivalent (I)
5.6	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (I)
5.7	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (I)
5.8	Attack: Release of Infectious Agents (I)
5.9	Civil Disorder (I)
5.10	Sabotage (I)
5.11	Theft (I)
5.12	Trespassing (O)
5.13	Vandalism (I)
5.14	Vehicle as a Weapon (I)

Asset-Threat Combinations (Outsider/Insider)	
6	Cargo Facilities
6.1	Armed Attack (I)
6.2	Arson (I)
6.3	Assault (I)
6.4	Attack: Explosives <=5kg TNT Equivalent (I/O)
6.5	Attack: Explosives <=15kg TNT Equivalent (I/O)
6.6	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (I/O)
6.7	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (I/O)
6.8	Attack: Release of Infectious Agents (I)
6.9	Civil Disorder (I)
6.10	Sabotage (I)
6.11	Theft (I/O)
6.12	Trespassing (O)
6.13	Vandalism (I)
6.14	Vehicle as a Weapon (I)
7	Catering Facilities
7.1	Armed Attack (I)
7.2	Attack: Release of Infectious Agents (I)
7.3	Sabotage (I)
7.4	Theft (I)
7.5	Vandalism (I)
8	Checked Baggage Screening/Operations/Makeup Areas
8.1	Armed Attack (I)
8.2	Arson (I)
8.3	Assault (I)
8.4	Attack: Explosives <=5kg TNT Equivalent (I)
8.5	Attack: Explosives <=15kg TNT Equivalent (I)
8.6	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (I)
8.7	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (I)
8.8	Attack: Release of Infectious Agents (I)
8.9	Sabotage (I)
8.10	Theft (I)
8.11	Vandalism (I)
8.12	Vehicle as a Weapon (I)
9	Concession Storage Areas
9.1	Attack: Release of Infectious Agents (I)
9.2	Sabotage (I)
9.3	Theft (I)
9.4	Vandalism (I)
10	Deicing Systems
10.1	Sabotage (I)
10.2	Vandalism (I)
11	Federal Inspection Stations
11.1	Armed Attack (I)
11.2	Arson (I)
11.3	Assault (I)
11.4	Attack: Explosives <=5kg TNT Equivalent (I)
11.5	Attack: Explosives <=15kg TNT Equivalent (I)
11.6	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (I)
11.7	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (I)

Asset-Threat Combinations (Outsider/Insider)
11.8 Attack: Release of Infectious Agents (I)
11.9 Civil Disorder (I)
11.10 Sabotage (O/I)
11.11 Vandalism (I)
12 Fuel Farm
12.1 Armed Attack (I)
12.2 Arson (I)
12.3 Assault (I)
12.4 Attack: Explosives <=5kg TNT Equivalent (I)
12.5 Attack: Explosives <=15kg TNT Equivalent (I)
12.6 Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (I)
12.7 Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (I)
12.8 Civil Disorder (I)
12.9 Sabotage (I)
12.10 Theft (I)
12.11 Trespassing (O)
12.12 Vandalism (I)
12.13 Vehicle as a Weapon (I)
13 General/Business Aviation Areas
13.1 Armed Attack (I)
13.2 Arson (I)
13.3 Assault (I)
13.4 Attack: Explosives <=5kg TNT Equivalent (I/O)
13.5 Attack: Explosives <=15kg TNT Equivalent (I/O)
13.6 Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (I/O)
13.7 Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (I/O)
13.8 Sabotage (I/O)
13.9 Theft (I/O)
13.10 Vandalism (I/O)
13.11 Vehicle as a Weapon (I/O)
14 Ground Run-up Enclosure
14.1 Attack: Explosives <=5kg TNT Equivalent (I)
14.2 Attack: Explosives <=15kg TNT Equivalent (I)
14.3 Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (I)
14.4 Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (I)
14.5 Sabotage (I)
14.6 Vandalism (I)
14.7 Vehicle as a Weapon (I)
15 Jet-bridge Access
15.1 Armed Attack (I)
15.2 Arson (I)
15.3 Attack: Explosives <=5kg TNT Equivalent (I)
15.4 Attack: Explosives <=15kg TNT Equivalent (I)
15.5 Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (I)
15.6 Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (I)
15.7 Attack: Release of Infectious Agents (I)
15.8 Sabotage (I)
15.9 Vandalism (I)
15.10 Vehicle as a Weapon (I)
16 Movement Areas (runways and taxiways)
16.1 Armed Attack (I)

Asset-Threat Combinations (Outsider/Insider)
16.2 Assault (I)
16.3 Attack: Explosives <=5kg TNT Equivalent (I)
16.4 Attack: Explosives <=15kg TNT Equivalent (I)
16.5 Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (I)
16.6 Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (I)
16.7 Sabotage (I)
16.8 Theft (I)
16.9 Trespassing (O/I)
16.10 Vandalism (I)
16.11 Vehicle as a Weapon (O/I)
17 Non-movement Area Vehicle Access Points
17.1 Armed Attack (I)
17.2 Assault (I)
17.3 Attack: Explosives <=5kg TNT Equivalent (I)
17.4 Attack: Explosives <=15kg TNT Equivalent (I)
17.5 Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (I)
17.6 Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (I)
17.7 Sabotage (I)
17.8 Theft (I)
17.9 Trespassing (I)
17.10 Vandalism (I)
17.11 Vehicle as a Weapon (O/I)
18 Perimeter Fencing
18.1 Attack: Explosives <=5kg TNT Equivalent (O/I)
18.2 Attack: Explosives <=15kg TNT Equivalent (O/I)
18.3 Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
18.4 Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
18.5 Sabotage (O/I)
18.6 Trespassing (O/I)
18.7 Vandalism (O/I)
18.8 Vehicle as a Weapon (O/I)
19 Perimeter Intrusion Detection System
19.1 Sabotage (O/I)
20 Vehicle Gates
20.1 Armed Attack (O/I)
20.2 Assault (I)
20.3 Attack: Explosives <=5kg TNT Equivalent (O/I)
20.4 Attack: Explosives <=15kg TNT Equivalent (O/I)
20.5 Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
20.6 Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
20.7 Civil Disorder (O/I)
20.8 Sabotage (O/I)
20.9 Trespassing (O/I)
20.10 Vandalism (O/I)
20.11 Vehicle as a Weapon (O/I)
B. Terminal Operations (Public)
1 Baggage Claim
1.1 Armed Attack (O/I)
1.2 Assault (O/I)
1.3 Attack: Explosives <=5kg TNT Equivalent (O/I)
1.4 Attack: Explosives <=15kg TNT Equivalent (O/I)

	Asset-Threat Combinations (Outsider/Insider)
1.5	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
1.6	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
1.7	Attack: Release of Infectious Agents (O/I)
1.8	Theft (O/I)
1.9	Vandalism (O/I)
2	Concessions
2.1	Armed Attack (O/I)
2.2	Assault (O/I)
2.3	Attack: Explosives <=5kg TNT Equivalent (O/I)
2.4	Attack: Explosives <=15kg TNT Equivalent (O/I)
2.5	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
2.6	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
2.7	Attack: Release of Infectious Agents (O/I)
2.8	Sabotage (I)
2.9	Theft (O/I)
2.10	Vandalism (I)
3	Security Screening Checkpoints
3.1	Armed Attack (O/I)
3.2	Assault (O/I)
3.3	Attack: Explosives <=5kg TNT Equivalent (O/I)
3.4	Attack: Explosives <=15kg TNT Equivalent (O/I)
3.5	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
3.6	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
3.7	Attack: Release of Infectious Agents (O/I)
3.8	Civil Disorder (O/I)
3.9	Sabotage (I)
3.10	Vandalism (I)
4	Ticket Counters/Automated Check-in Areas
4.1	Armed Attack (O/I)
4.2	Arson (O/I)
4.3	Assault (O/I)
4.4	Attack: Explosives <=5kg TNT Equivalent (O/I)
4.5	Attack: Explosives <=15kg TNT Equivalent (O/I)
4.6	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
4.7	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
4.8	Attack: Release of Infectious Agents (O/I)
4.9	Civil Disorder (O/I)
4.10	Sabotage (O/I)
4.11	Vandalism (O/I)
C.	**Landside Operations**
1	General Traffic/Curbside Management Operations
1.1	Armed Attack (O/I)
1.2	Attack: Explosives <=5kg TNT Equivalent (O/I)
1.3	Attack: Explosives <=15kg TNT Equivalent (O/I)
1.4	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
1.5	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
1.6	Attack: Release of Infectious Agents (O/I)
1.7	Civil Disorder (O/I)
1.8	Sabotage (O/I)
1.9	Vehicle as a Weapon (O/I)
2	Ground Transportation Operations

	Asset-Threat Combinations (Outsider/Insider)
2.1	Armed Attack (O/I)
2.2	Attack: Explosives <=5kg TNT Equivalent (O/I)
2.3	Attack: Explosives <=15kg TNT Equivalent (O/I)
2.4	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
2.5	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
2.6	Attack: Release of Infectious Agents (O/I)
2.7	Civil Disorder (O/I)
2.8	Sabotage (O/I)
2.9	Theft (O/I)
2.10	Vehicle as a Weapon (O/I)
3	Parking Operations
3.1	Armed Attack (O/I)
3.2	Attack: Explosives <=5kg TNT Equivalent (O/I)
3.3	Attack: Explosives <=15kg TNT Equivalent (O/I)
3.4	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
3.5	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
3.6	Attack: Release of Infectious Agents (O/I)
3.7	Civil Disorder (O/I)
3.8	Sabotage (O/I)
3.9	Vehicle as a Weapon (O/I)
4	Rental Car Operations
4.1	Armed Attack (O/I)
4.2	Theft (O/I)
D.	**Infrastructure**
1	Airport Authority Administrative Offices
1.1	Armed Attack (O/I)
1.2	Arson (O/I)
1.3	Sabotage (O/I)
1.4	Vandalism (O/I)
2	Airport Authority Ground Vehicle Fueling Systems
2.1	Arson (O/I)
2.2	Attack: Explosives <=5kg TNT Equivalent (O/I)
2.3	Attack: Explosives <=15kg TNT Equivalent (O/I)
2.4	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
2.5	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
2.6	Sabotage (O/I)
2.7	Theft (O/I)
2.8	Vandalism (O/I)
2.9	Vehicle as a Weapon (O/I)
3	Audio Communications Systems
3.1	Sabotage (O/I)
3.2	Theft (O/I)
3.3	Vandalism (O/I)
4	Cellular Communications Systems
4.1	Sabotage (O/I)
4.2	Theft (O/I)
4.3	Vandalism (O/I)
5	Common Use Information Technology/Networks
5.1	Sabotage (O/I)
5.2	Theft (O/I)

	Asset-Threat Combinations (Outsider/Insider)
5.3	Vandalism (O/I)
6	Dispatch/Communications Centers
6.1	Armed Attack (I)
6.2	Sabotage (O/I)
6.3	Theft (O/I)
6.4	Vandalism (O/I)
7	Electrical Power Systems
7.1	Sabotage (O/I)
7.2	Theft (O/I)
7.3	Vandalism (O/I)
8	First Responder Communications Systems
8.1	Sabotage (O/I)
8.2	Theft (O/I)
8.3	Vandalism (O/I)
9	Heating, Ventilation, and Air Conditioning (HVAC) Systems
9.1	Attack: Release of Infectious Agents (O/I)
9.2	Sabotage (O/I)
9.3	Theft (O/I)
9.4	Vandalism (O/I)
10	Law Enforcement Facilities and Resources
10.1	Armed Attack (O/I)
10.2	Arson (O/I)
10.3	Attack: Explosives <=5kg TNT Equivalent (O/I)
10.4	Attack: Explosives <=15kg TNT Equivalent (O/I)
10.5	Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
10.6	Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
10.7	Attack: Release of Infectious Agents (O/I)
10.8	Sabotage (O/I)
11	Mechanical, Electrical, Plumbing (MEP)
11.1	Sabotage (O/I)
11.2	Theft (O/I)
11.3	Vandalism (O/I)
12	Natural Gas Services
12.1	Sabotage (O/I)
12.2	Theft (O/I)
12.3	Vandalism (O/I)
13	Potable Water Services
13.1	Attack: Release of Infectious Agents (O/I)
13.2	Sabotage (O/I)
13.3	Theft (O/I)
13.4	Vandalism (O/I)
14	Radio Communications Systems
14.1	Sabotage (O/I)
14.2	Theft (O/I)
14.3	Vandalism (O/I)
15	Sewer Systems
15.1	Sabotage (O/I)
15.2	Theft (O/I)
15.3	Vandalism (O/I)

Asset-Threat Combinations (Outsider/Insider)
16 Storm Water Systems
16.1 Sabotage (O/I)
16.2 Theft (O/I)
16.3 Vandalism (O/I)
17 Vendor Deliveries
17.1 Civil Disorder (O/I)
17.2 Sabotage (O/I)
17.3 Theft (O/I)
17.4 Vandalism (O/I)
18 Vertical Circulation Systems
18.1 Armed Attack (O/I)
18.2 Arson (O/I)
18.3 Attack: Explosives <=5kg TNT Equivalent (O/I)
18.4 Attack: Explosives <=15kg TNT Equivalent (O/I)
18.5 Attack: Explosives <=500Kg TNT Equivalent – Small VBIED (O/I)
18.6 Attack: Explosives >=500Kg TNT Equivalent – Large VBIED (O/I)
18.7 Attack: Release of Infectious Agents (O/I)
18.8 Sabotage (O/I)
18.9 Vandalism (O/I)
19 Video Communications Systems
19.1 Sabotage (O/I)
19.2 Theft (O/I)
19.3 Vandalism (O/I)
20 Video Surveillance Systems
20.1 Sabotage (O/I)
20.2 Theft (O/I)
20.3 Vandalism (O/I)
21 Waste Management Systems
21.1 Sabotage (O/I)
21.2 Vandalism (O/I)

C4 – Consequence Analysis Tool

Table C-7 is an example of a consequence analysis tool that can be applied to small, medium, or large hub airports. The tool can be used to document use of proxy measures provided in the SVA Tools (Tab 4.1) or use of alternative estimates derived by the SVA team. Alternative estimates can be entered into the SVA Tool to yield risk results.

Note: Data entered into Tab 4.1 in the SVA Tools automatically calculates consequences in Tabs 4.2 and 4.3. Consequences for each threat estimated in Tab 4.3 are used to calculate total risk in Tabs 7.1 and 7.2.

Instructions: The cells highlighted yellow indicate where proxy measures can be found in the SVA Tools. These proxy measures can be modified. If an alternative estimate is used, enter "Yes" in the column "Alternative Value Used."

Table C-7. Consequence Analysis Tool

Components/Sub-components	Rate	Proxy Estimate	Suggestions	Alternative Value Used? (yes or no)
Fatalities				
Loss Estimate per Fatality	---		To be determined in consultation with airport management, local emergency management, or other source.	
Traffic per Day	---		Use FAA data as an average for small/medium/large hub airports (enplanements+deplanements adjusted for yearly increase) or substitute local data if available.	
Hours of Operation			Adjust for average hours of operation/day.	
Average Number of Patrons per Hour	---		Patrons per hour based on hours/operating day.	
Estimated Fatalities (based on percent impacted by attack type)				
Armed Attack			Fatality rates based on attack type are based on experiential data. No other sources of data are known. Estimates are consistent with known events. Use alternative value in consultation with subject matter experts.	
Arson				
Assault				
Attack: Explosives <=5kg TNT Equivalent				
Attack: Explosives <=15kg TNT Equivalent				
Attack: Explosives <=500Kg TNT Equivalent –Small VBIED				
Attack: Explosives >=500Kg TNT Equivalent – Large VBIED				
Attack: Release of Infectious Agents				
Civil Disorder/ Protest				
Sabotage				

Components/Sub-components	Rate	Proxy Estimate	Suggestions	Alternative Value Used? (yes or no)
Theft				
Trespassing				
Vandalism				
Vehicle as a Weapon				
Injuries				
Loss Estimate per Injury	---		To be determined in consultation with airport management, local emergency management, or other source.	
Traffic per Day	---		Use FAA data as an average for small/medium/large hub airports (enplanements+deplanements adjusted for yearly increase) or substitute local data if available.	
Average Number of Patrons per Hour			Adjust for average hours of operation/day.	
Estimated Injuries (based on percent impacted by attack type)	---		Patrons per hour based on hours/operating day.	
Armed Attack			Injury rates based on attack type are based on experiential data. No other sources of data are known. Estimates are consistent with known events. Use alternative value in consultation with subject matter experts.	
Arson				
Assault (manual input; not based on percent)				
Attack: Explosives <=5kg TNT Equivalent				
Attack: Explosives <=15kg TNT Equivalent				
Attack: Explosives <=500Kg TNT Equivalent –Small VBIED				
Attack: Explosives >=500Kg TNT Equivalent – Large VBIED				
Attack: Release of Infectious Agents				
Civil Disorder/ Protest				
Sabotage				
Theft				
Trespassing				
Vandalism				
Vehicle as a Weapon				
Displacement/Workaround Cost				
Displacement/Workaround Cost ($ per square foot/month)	---		Recognized government standard Substitute if local emergency management agencies or other local government have an alternative cost estimate.	
Estimated Area Impacted by Threat (square feet)				

Components/Sub-components	Rate	Proxy Estimate	Suggestions	Alternative Value Used? (yes or no)
Armed Attack	---		The sizes of areas impacted by various attack types are based on experiential data. No other sources of data are known. Estimates are consistent with known events.	
Arson	---			
Assault	---			
Attack: Explosives <=5 kg TNT Equivalent	---			
Attack: Explosives <=15 kg TNT Equivalent	---			
Attack: Explosives <=500 kg TNT Equivalent, Small VBIED	---			
Attack: Explosives >=500 kg TNT Equivalent, Large VBIED	---			
Attack: Release of Infectious Agents	---			
Civil Disorder/ Protest	---			
Sabotage	---			
Theft	---			
Trespassing	---			
Vandalism	---			
Vehicle as a Weapon	---			
Estimated Time of Displacement/Workaround (months)				
Armed Attack	---		The timelines (months) for displacement/workaround for various attack types are based on experiential data. No other sources of data are known. Estimates are consistent with known events.	
Arson	---			
Assault	---			
Attack: Explosives <=5 kg TNT Equivalent	---			
Attack: Explosives <=15 kg TNT Equivalent	---			
Attack: Explosives <=500 kg TNT Equivalent, Small VBIED	---			
Attack: Explosives >=500 kg TNT Equivalent, Large VBIED	---			
Attack: Release of Infectious Agents	---			
Civil Disorder/ Protest	---			
Sabotage	---			
Theft	---			
Trespassing	---			
Vandalism	---			
Vehicle as a Weapon	---			
Replacement/Repair Cost				

Components/Sub-components	Rate	Proxy Estimate	Suggestions	Alternative Value Used? (yes or no)
Replacement/Repair Cost ($ per square feet)	---		Average per square foot construction cost of $200 is based on a recognized source. Local data/building type data may vary. If a different value is used based on local conditions, FEMA recommends doubling the number to account for content value.	
Estimated Area Impacted (square feet)				
Armed Attack			The sizes of areas impacted by various attack types are based on experiential data. No other sources of data are known. Estimates are consistent with known events.	
Arson				
Assault				
Attack: Explosives <=5 kg TNT Equivalent				
Attack: Explosives <=15 kg TNT Equivalent				
Attack: Explosives <=500 kg TNT Equivalent, Small VBIED				
Attack: Explosives >=500 kg TNT Equivalent, Large VBIED				
Attack: Release of Infectious Agents				
Civil Disorder/ Protest				
Sabotage				
Theft				
Trespassing				
Vandalism				
Vehicle as a Weapon				
Loss of Service Cost to Airport				
Loss of Service Cost per Passenger	---		Based on recognized government statistics. Local statistics can be substituted if available.	
Estimated Loss of Service Time (days)				
Armed Attack	---		Estimated loss of service times for various attack types are based on experiential data. No other sources of data are known. Estimates are consistent with known events. Note: Estimates are those used for Displacement/Workaround Costs converted from months to days.	
Arson	---			
Assault	---			
Attack: Explosives <=5 kg TNT Equivalent	---			
Attack: Explosives <=15 kg TNT Equivalent	---			
Attack: Explosives <=500 kg TNT Equivalent, Small VBIED	---			
Attack: Explosives >=500 kg TNT Equivalent, Large VBIED	---			
Attack: Release of Infectious Agents	---			

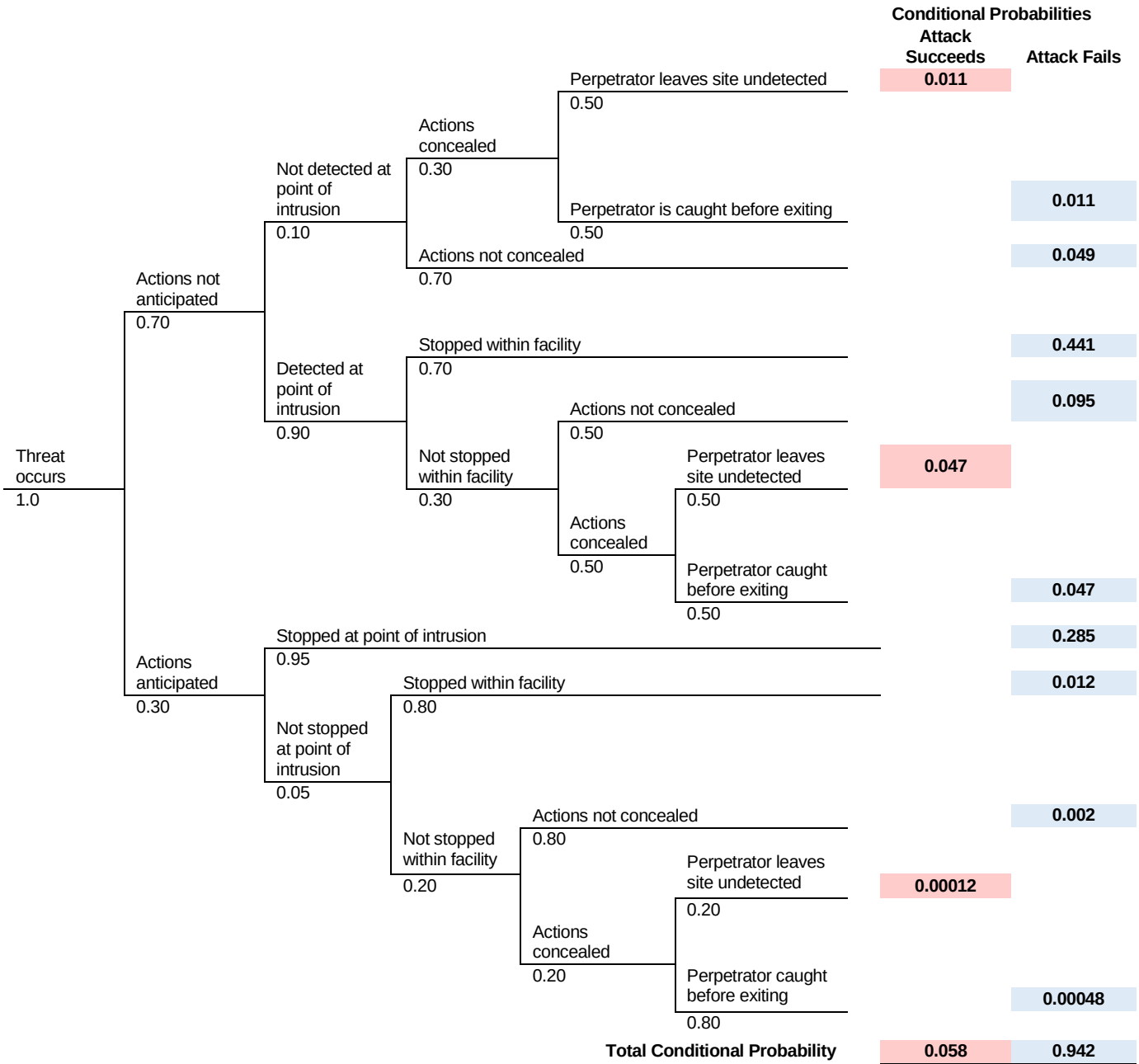
Components/Sub-components	Rate	Proxy Estimate	Suggestions	Alternative Value Used? (yes or no)
Civil Disorder/ Protest	---			
Sabotage	---			
Theft	---			
Trespassing	---			
Vandalism	---			
Vehicle as a Weapon	---			
Percent of Airport Impacted				
Armed Attack	---		Percent of airport impacted by attack type is based on experiential data. No other sources of data are known. Estimates are consistent with known events. Total Loss of Service Cost = $211/passenger x 5,886 passengers/day x Estimated Loss of Service Time (days) x Percent of Airport Impacted.	
Arson	---			
Assault	---			
Attack: Explosives <=5 kg TNT Equivalent	---			
Attack: Explosives <=15 kg TNT Equivalent	---			
Attack: Explosives <=500 kg TNT Equivalent, Small VBIED	---			
Attack: Explosives >=500 kg TNT Equivalent, Large VBIED	---			
Attack: Release of Infectious Agents	---			
Civil Disorder/ Protest	---			
Sabotage	---			
Theft	---			
Trespassing	---			
Vandalism	---			
Vehicle as a Weapon	---			
Loss Due to Theft				
Average Loss Per Theft ($)	---		Based on 2018 National Retail Security Survey, National Retail Federation, Page 12, https://cdn.nrf.com/sites/default/files/2018-10/NRF-NRSS-Industry-Research-Survey-2018.pdf.	
Average Theft Rate (4.195/100,000)	---		Based on research conducted at Rutgers University, https://rucore.libraries.rutgers.edu/rutgers-lib/39449/PDF/1/play/.	

C5 – Vulnerability Analysis Tools – Example Event Trees

Event trees are used to assess the pathways for malevolent threats to occur and their relative probabilities. A probability is assigned to each event in a path, and then the probabilities for all events in a single path are multiplied to calculate the conditional probability of the attack failing or succeeding.

Figure C-1 shows an example structure of an event tree for an attack on an airport location. See Tab XX in the SVA Tools for event trees that apply to specific threat-asset combinations and corresponding proxy estimates. The SVA team may use these event trees as provided or as a basis for developing their own vulnerability estimates. The SVA team should engage law enforcement, airport security experts, and other SMEs to review and revise proxy measures if there is reason to believe that conditions at a specific airport may vary.

Figure C-1. Example Event Tree



APPENDIX D: CYBERSECURITY CONSIDERATIONS

While statistics in the United States are difficult to find, the European Aviation Safety Agency estimates that 1,000 cyberattacks occur monthly on aviation systems.[49] Successful penetration of airport systems has occurred within the United States. Following the same steps as described in the body of this guidance document, this appendix provides general guidance for performing a cybersecurity risk assessment. Information below is intended to provide a starting point for assessing cybersecurity risks. It is recommended that all parameters be validated and evaluated by qualified information technology and cybersecurity experts.

D1 – Cyber/IT Assets

Table D-1 provides a list of cyber/information technology assets that may be susceptible to malevolent threats. IT/cybersecurity experts should validate the list of assets and contract or expand as needed.

Table D-1. Cyber/IT Asset Register

	IT Network Infrastructure and Services
1	Active Directory
2	Anti-Virus
3	Backup Services
4	Cellular Data Network
5	Document Management/File Share
6	E-Mail Hardware
7	E-Mail Software
8	Internet Hardware
9	Internet Software
10	Leased Lines
11	Log Management
12	Patch Management
13	Physical Security Services
14	Remote Access
15	Telemetry
16	Virtualization
17	WAN Cabling
18	WAN Routing
	Vendors
1	Cellular Providers
2	Contractors
3	Internet Provider(s)

	IT Operations and Business Continuity
1	Business Continuity Plan
2	Data Backup Strategy
3	Disaster Recovery Plan
4	Generator(s)
5	Hardware Standards (Server, Desktop, Network, etc.)
6	Networking
7	Power Feed
8	Programmable Logic Controllers (PLCs)
9	SCADA Primary/Secondary Servers
10	SCADA Software
11	SCADA Workstations
12	Software Standards
13	Telemetry
14	Uninterruptible Power Supply (UPS)
	Applications
1	Control/Operations Center Hardware
2	Control/Operations Center Software
3	Financial Information System Hardware
4	Financial Information System Software
5	Geographic Information System (GIS) Hardware
6	GIS Software
7	Timekeeping Hardware
8	Timekeeping Software

[49] https://www.euractiv.com/section/justice-home-affairs/news/hackers-bombard-aviation-sector-with-more-than-1000-attacks-per-month/

In addition to critical assets, identifying critical internal and external supporting infrastructures and their interdependencies facilitates assessment of their impact on resiliency. Particular attention should be paid to critical assets that are single points of failure (i.e., an electrical substation that is the sole electrical supply). Examples include:

- **Electrical Utilities** – IT and SCADA systems cannot run without continuous electrical power. Though Uninterruptible Power Supply (UPS) units and diesel generators can, if properly configured, maintain continuous power as long as fuel is supplied, their intended use is to provide power for hours or days.
- **Employees/Other Experts** – SMEs, whether airport employees, concessionaires, or contractors, are key to reconstituting airport cyber infrastructure in the aftermath of a disaster. Such expertise may extend to remote contracts including specialized expertise from outside the United States.
- **Fuel** – Related to the dependency on electrical utilities, diesel fuel sources are needed to run generators in the case of a power failure. Though typical on-site fuel capacity is adequate for extended run periods, larger capacity generators can consume over 100 gallons of diesel fuel an hour at full load. Due to likely strains on fuel supplies during a regional emergency, this solution cannot be relied upon to supply electrical power indefinitely.
- **Telecommunications** – Many airports rely on wide area networks for internet/intranet services, e-mail, and other distributed enterprise applications. An outage in the telecommunications system could significantly affect airport operations during an extend outage.
- **Vendors** – If critical IT infrastructure is rendered inoperable for any reason, hardware, software, and other vendors may be relied upon to deliver appropriate devices within negotiated timeframes to ensure continuity of airport business functions.

D2 – Cyber/IT Threats

The ACRP document Guidebook on Best Practices for Airport Cybersecurity[50] contains a detailed categorized list of cybersecurity threats. The most common malevolent attacks against IT assets include:

1. Hacking – Outsider/Insider
2. Sabotage – Outsider/Insider
3. Theft – Outsider/Insider

Various means of delivery regarding cyber threats may include, but are not limited to:

1. Internet/intranet hacking
2. Wi-Fi intrusion
3. Intrusion via hand-held media (CDs, USB flash drives, etc.)
4. Physical destruction (explosives or other physical intrusion)

The extent of the impact of malevolent threats, and mitigation strategies to reduce specific cyber threats, should consider characteristics of potential adversaries relative to each malevolent threat. Adversaries may include:

1. Political or terrorist groups (driven by a cause)
2. Computer Hackers (less cause-driven and more thrill-seeking)
3. Criminals (driven by financial or other gain)
4. Rogue employees/former employees (driven by revenge)

[50] Airport Cooperative Research Program, Guidebook on Best Practices for Airport Cybersecurity, Appendix A, Categorized List of Cybersecurity Threats, pages 80–88, 2015.

Airport staff should be constantly vigilant and aware of external adversaries who attempt to purchase inside information or gain inside information of potential weaknesses in cyber systems. Airport management should also remain vigilant regarding potential disgruntled employee job actions or intentional sabotage of equipment and security technology systems. Employee malevolent acts may include:

1. Intentional equipment sabotage/workplace violence
2. Selling/giving information to external adversaries
3. Theft or embezzlement
4. Enabling "portals" into airport IT networks such as authorized Wi-Fi installations

Understanding the types of cyber-threats, the potential means to unleash a threat, and motivations behind threats allows full threat characterization, assessment of risk, and identification of possible mitigation strategies.

D3 – Consequences

Estimating potential consequences of threats applied to cyber assets generally focuses on the following elements:

- Costs of injuries or fatalities, if applicable
- Repair and replacement costs for assets damaged or destroyed including escalation costs for expedited construction/installation
- Business interruption costs including any liability costs for service interruption
- Remediation and other liability costs
- Length of time service is denied

Examples of worst reasonable case assumptions for evaluating asset-threat combinations are provided in Table D-2.

Table D-2. Examples of Cyber Asset-Threat Combinations Worst Reasonable Cases

Asset-Threat Combination	Worst Reasonable Cases
SCADA/Other Control System – Hacker	Process disruption; unattended workstation or other means used to gain access to SCADA or other control system and execute an adverse scenario. Worst case likely involves critical airfield systems or communications systems.
Internal Network – Hacker	Internal network security circumvented; inside hacker can exploit vulnerability to compromise applications. IT would investigate the breach, trace back to entry point, and shut it off while keeping the network running. Worst case, some virus/worm attacks can discontinue operations for a day.
External Network Security (Internet) – Hacker	External network security circumvented; hacker can exploit vulnerability to compromise enterprise applications. IT would investigate the breach, trace back to entry point, and shut it off while keeping the network running. Worst case, some virus/worm attacks can discontinue operations for a day.
Data Center Capability – Hacker with Physical Access	Extensive IT system compromise; may take additional time to recover without a disaster recovery/business continuity plan in place. Potential exists to unplug or physically render inoperable. Generally, downtime duration is likely to be 12 hours to 7 days.
Financial Applications – Hacker	System compromised; extensive compromise of customer information. Worst case is an approximate 72-hour rebuild timeframe.

Asset-Threat Combination	Worst Reasonable Cases
Website – Hacker	Website vandalized or rendered inoperative; disrupts internet transactions for up to a week and may interrupt communications features. Alternate site development requires a very short time to put into place.
Control Center – Hacker	Control Center software compromised; potential sensitive information exposed and critical systems compromised. Programming resources on-site to rebuild or activate "test cluster" backup system at a backup location if fully compromised. Similarly, back-end is running at two different locations for redundancy. IT staff institutes several levels of code review.

Worst-case scenarios can be used to quantify economic impacts based on down time and other parameters identified during consequence analysis.

D4 – Probability

As with other threats, determining the probability of a cyber threat occurring is a function of available intelligence, objectives and capabilities of the adversary, and the attractiveness, or symbolic or fear-inducing value of the asset as a target. Ultimately, probability is a measure of the frequency that a particular event will occur in a defined period.

Because cyber threats are dynamic, it is difficult to obtain up-to-date intelligence information to support estimations of a specific threat probability. To develop best estimates of probability, it is recommended that cyber industry experts be consulted to arrive at a consensus for each type of cyber threat. In addition to the very nature of how cyber threats occur, other considerations should include the frequency of threat occurrence in the United States, if available, and the perceived attractiveness of the target. Airports in larger cities may be more attractive to a perpetrator with terrorist motives. However, airports and other critical infrastructure in small towns have not been immune to cyberattacks.

The purpose of estimating probability as a function of risk is to prioritize those threats that are most likely to occur. Thus, if data is lacking, it is acceptable to assign a relative ranking to each cyber threat based on expert consensus. Sources of expertise may include internal IT staff, other local government agencies (city/county IT and/or emergency management agency), and the National Institute of Standards and Technology.[51] As with other hazards, assigned probability should be between zero (0) and one (1) with least-likely threats assigned a value closer to zero and most-likely threats assigned a value closer to one.

D5 – Vulnerability

Vulnerability relative to cyber assets is the inherent state of a system (physical, technical, organizational, or cultural) that can be exploited by an adversary to cause harm or damage. Such weaknesses can include:

- System characteristics
- Equipment properties
- Personnel behavior
- Location of people, equipment, or systems
- Operational and personnel practices

[51] https://www.nist.gov/topics/cybersecurity

Estimating vulnerability should include:

1. Review of pertinent details of systems, procedures, and features including:
    a. Countermeasures, mitigation measures, and other impediments designed to protect cyber systems
    b. Equipment features that provide deterrence, detection, or delay devices
    c. Local supporting response measures
    d. Information regarding interdependencies, personal interactions, and process flows
2. Vulnerability analysis of each critical cyber asset or system to estimate the likelihood that a given threat will result in predicted consequences
3. Estimation of vulnerability using event trees or other methods

Event trees analyze the sequence of events between initiation of a cyberattack and the terminal event in the form of a branched bracket where each branch represents the possible outcomes at that junction, such as a firewall being breached or not breached. The probability of each outcome is estimated and those probabilities are multiplied, along each branch, from the initiating event to each terminal event. The ultimate calculation provides the probability of each unique branch with all branches together summing to unity (1.0). The sum of the probabilities of all branches on which an attack succeeds is the vulnerability estimate.

Figure D-1. Example Event Tree: Cybersecurity Threat-Insider

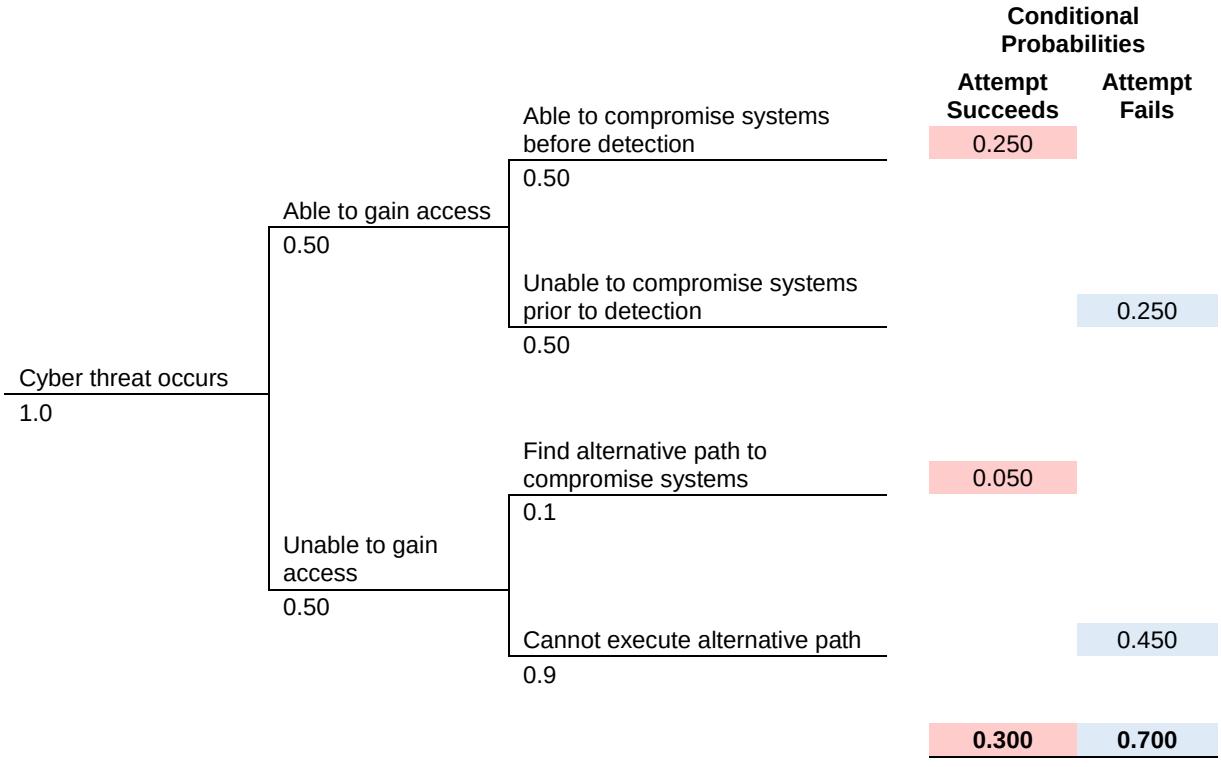
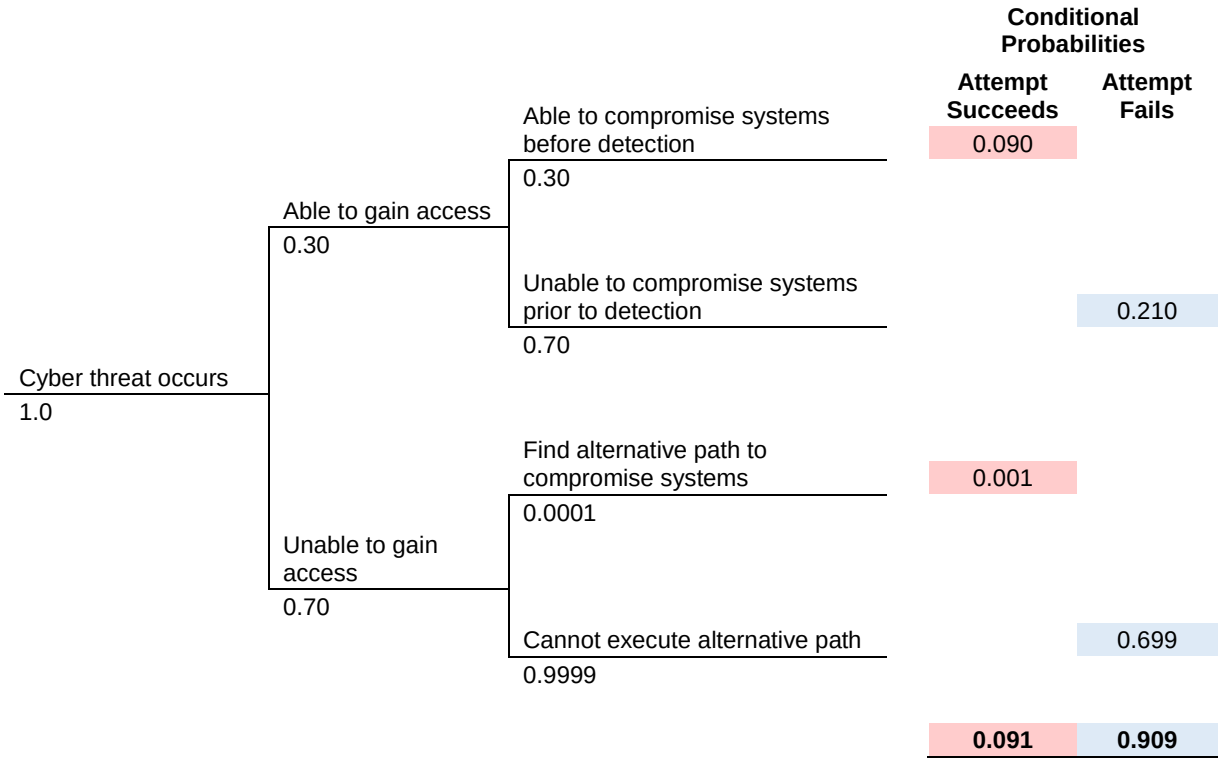


Figure D-2. Example Event Tree: Cybersecurity Threat-Outsider



Having identified consequence, threat probability, and asset vulnerabilities, risk for various asset-cyber threat combinations can be calculated.

D6 – Cybersecurity Risk Mitigation

Upon determining and prioritizing risk for various asset-cyber threat combinations, mitigation measures can be identified. Examples of cyber risk mitigation measures are described below.

Control systems and information technology systems, such as email, should be provided with all standard cybersecurity components such as firewalls and demilitarized zones. In addition, basic policies and procedures, as outlined in industry standards such as the International Society of Automation (ISA)-99, Security Technologies for Industrial Automation and Control Systems, and National Institute of Standards and Technology (NIST) 800 should be implemented. Additional conditional recommendations include:

- Create an access control policy and supporting security procedures for IT systems. In addition to configuring IT systems with advanced security features, a policy and accompanying procedures should be developed to ensure that only qualified personnel can access IT systems. Follow NIST Special Publication 800-82, "Guide to Industrial Control Systems Security, Section 5, Network Architecture," or other recognized standard as a reference to current best practices.
- Acquire and configure redundant servers for critical systems, as needed, to serve as emergency servers in case control rooms are compromised due to natural hazards or malicious incident. Spare servers provide flexibility to deploy technology-based capabilities to resume or maintain automated operations to the extent allowable by conditions. An SOP should be developed to guide staff through the steps to deploy and "promote" backup servers in emergency situations.

- Provide secure enclosures to physically segregate servers, UPS, and networking devices. Best practice is to segregate sensitive IT equipment from unauthorized access. A low-cost option provides for a mesh type enclosure with an access-controlled entry door.
- Require unique passwords to associate individual employees with any change from the IT system. This requirement can be enforced by the IT access control policy. Train personnel not to share passwords or credential information. Software employed at most airports can be accurately customized to accommodate these security provisions.
- Maintain a service contract with a firm capable of providing local industrial control technical support, perform penetration testing, and implement a Network Access Control (NAC) solution as needed. Penetration testing can reveal vulnerabilities to unauthorized access. A NAC solution can provide role-based access control, security policy enforcement, and guest access management.
- Ensure that control room/data centers are capable of withstanding natural hazard threats. Control rooms/data centers serve as critical information assets. Consideration should be given to placement of backup power generators to ensure resiliency.
- Request DHS to perform a cybersecurity audit periodically. Local emergency management agencies may support requests for cybersecurity audits to be conducted by DHS.

Other specific recommendations may be identified through assessment of cyber threats. Open sources for cybersecurity recommendations include:

- National Security Agency: https://www.nsa.gov/what-we-do/cybersecurity/#professional-resources
- SANS Institute, Information Security Resources: https://www.sans.org/security-resources/
- DHS Transportation Systems Sector Cybersecurity Framework Implementation Guide: https://www.dhs.gov/publication/tss-cybersecurity-framework-implementation-guide#

Significant private-sector resources are also available to support cybersecurity risk assessment and mitigation.

APPENDIX E: NATURAL HAZARD CONSIDERATIONS

Increasingly, airports are contending with significant natural hazards including earthquakes, flooding, hurricanes, tornadoes, and other forms of inclement weather. Following the same steps as described in the body of this guidance document, this appendix provides general guidance for assessing risks associated with natural hazards. In some cases, data sources for natural hazards are much more robust and provide a greater level of predictability than malevolent threats.

E1 – Assets and Hazards

Generally, assets to be considered when assessing hazards are similar to those assessed relative to malevolent threats. Reference hazards that may be considered are provided in Table F-1. The four most common natural hazards include earthquake, flood, hurricane, and tornado/wind; however, location-specific hazards should be identified and considered based on historical records.

Table E-1. Reference Hazards

Hazards	
Avalanche	Hurricane
Blizzard	Ice Storm
Drought	Landslide/Mudslide
Earthquake	Tornado/Wind
Extreme Cold/Heat	Tsunami
Flooding	Wildfire

E2 – Consequences

Estimating potential consequences of natural hazards should focus similar elements as other threats including:

- Costs of injuries or fatalities, if applicable
- Repair and replacement costs for assets damaged or destroyed including escalation costs for expedited construction/installation
- Business interruption costs including any liability costs for service interruption
- Remediation and other liability costs
- Length of time service is denied

Assessing these elements in relation to airport assets should utilize these assumptions:

1. Design Comparison – Only hazards that exceed the asset design implies risk. Thus, it is important to analyze design criteria (if available) of assets in relation to natural hazard intensity (Category for hurricanes, Fujita scale for tornadoes, etc.)
2. Relative Damage – If hazard intensity is greater than the design standard, damage increases with decreasing design standards
3. Estimated Impact – Impact is based on the expected magnitude of the hazard and the extent to which it exceeds the design of the asset.

Examples of worst reasonable case assumptions for evaluating asset-hazard combinations are provided in Table E-2.

Table E-2. Examples of Asset-Hazard Combinations Worst Reasonable Cases

Asset-Hazard Combinations	Worst Reasonable Cases
Electrical Switch Gear, Terminal X – Tornado	Destroyed; temporary generator will power until distribution equipment is replaced. Switchgear replacement minimum 8 weeks. No fatalities and two injuries.
Runway – Earthquake	Damage to one runway; can operate using alternate runway during repair (120 days). Significant cost; no fatalities or injuries.

Worst-case scenarios can be used to quantify economic impacts based on downtime and other parameters identified during consequence analysis.

E3 – Probability

Unlike many malevolent threats, substantial historical records exist for natural hazards, which assist greatly in identifying hazard probability. Probability analysis for natural hazards can be estimated utilizing frequencies by county from government and industry data sources normalized to a per year basis. Information sources that are useful in providing data used to support natural hazard probability analysis include:

- City/County Hazard Mitigation Plans – Required by FEMA, city/county hazard mitigation plans provide frequency data for locally relevant hazards
- National Oceanic and Atmospheric Administration (NOAA), Storm Prediction Center – Provides valuable information regarding hurricane, tornado, and other storm data (http://www.spc.noaa.gov/wcm/#jmc)
- U.S. Census Bureau, 2010 Census data for county areas in square miles supports probability analysis (https://www.census.gov/quickfacts/fact/table/US/PST045218)

Using this data, probability (frequency) for specific hazards can be established as indicate in Table E-3.

Table E-3. Example: Tornado Probabilities by County

County	Number of Events	Number of Years	Events/Year	County Area (sq. mile)	Probability (events/year/sq. mile)
County A	91	61	1.4918	709	0.0025
County B	82	61	1.3443	897	0.0018
County C	60	61	0.9836	539	0.0022

The purpose of estimating probability as a function of risk is to prioritize those hazards that are most likely to occur. Thus, if data is lacking, it is acceptable to assign a relative ranking to each hazard based on expert consensus. Sources of expertise may include local emergency management officials, public works, and other local government agencies. As with other hazards, assigned probability should be between zero (0) and one (1), with least-likely threats assigned a value closer to zero and most-likely threats assigned a value closer to one.

E4 – Vulnerability

Vulnerability of an asset is based on the design criteria of the asset that make it susceptible to damage or destruction by a natural hazard. Such weaknesses can include:

- Design basis of the asset
- Construction and system characteristics
- Asset/equipment properties
- Location of the asset

Estimating vulnerability should include:

1. Review of pertinent details of construction, systems, and features including design parameters, countermeasures, mitigation measures, and other hardening aspects designed to protect the asset from specific hazards

2. Vulnerability analysis of each critical asset or system to estimate the likelihood that a given hazard will result in predicted consequences
3. Estimation of vulnerability using event trees or other methods

Event trees analyze the sequence of events that occur due to a hazard in the form of a branched bracket, where each branch represents the possible outcomes at that junction. The probability of each outcome is estimated and those probabilities are multiplied, along each branch, from the initiating event to each terminal event. The ultimate calculation provides the probability of each unique branch with all branches together summing to unity (1.0). The sum of the probabilities of all branches on which an attack succeeds is the vulnerability estimate (attack succeeds) . Event trees for natural hazards differ from those developed for malevolent threats. The vulnerability of an asset to a natural hazard is established based on the design basis of the asset (i.e., was the asset developed to withstand a specific level of hazard?) Thus, the event trees for natural hazards are typically simplified as opposed to those developed for malevolent threats. Example event trees are provided in Figures E-1 and E-2 on the following pages.

Figure E-1. Example Event Tree: Tornado – Electrical Switch Gear, Terminal X

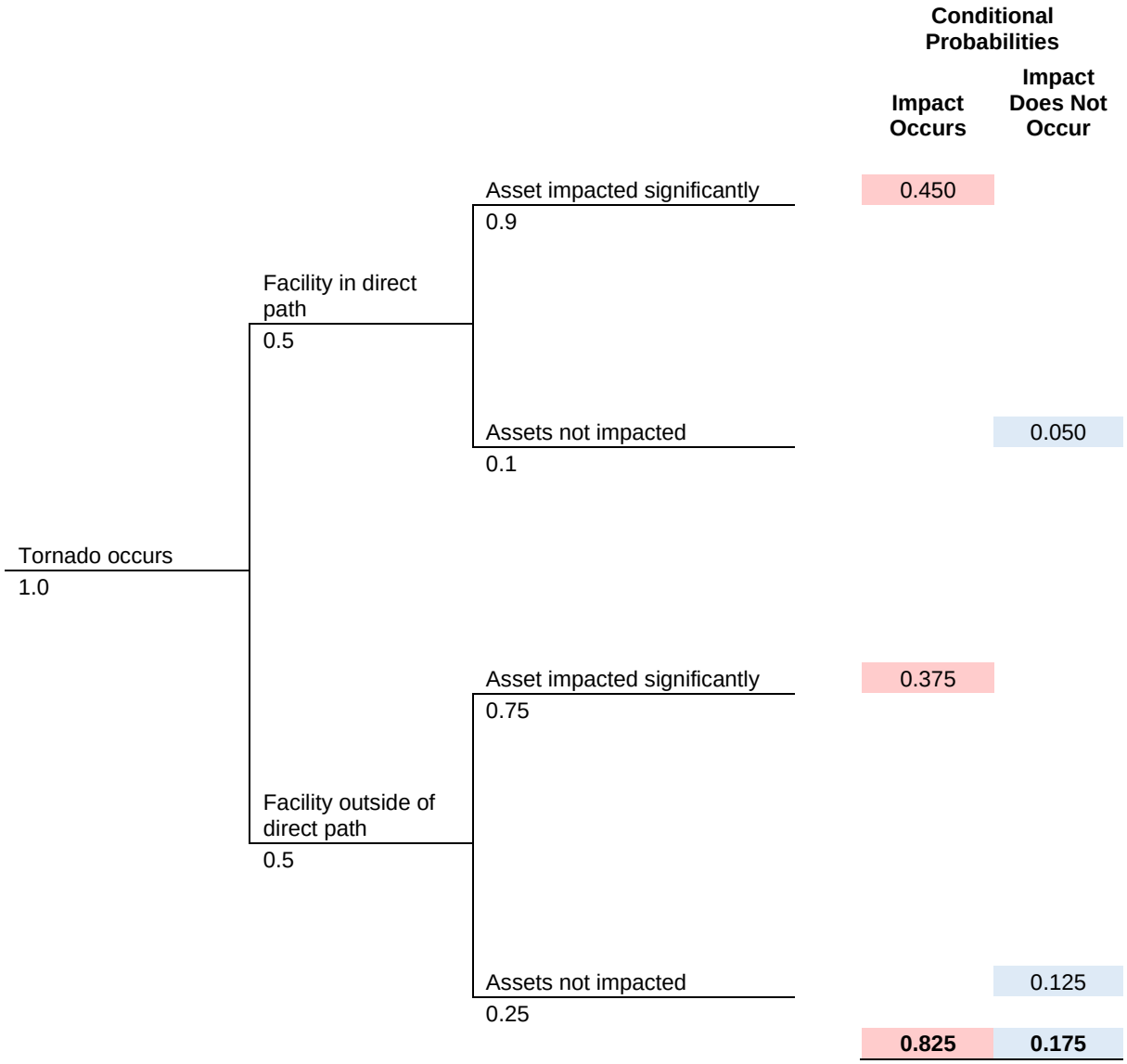
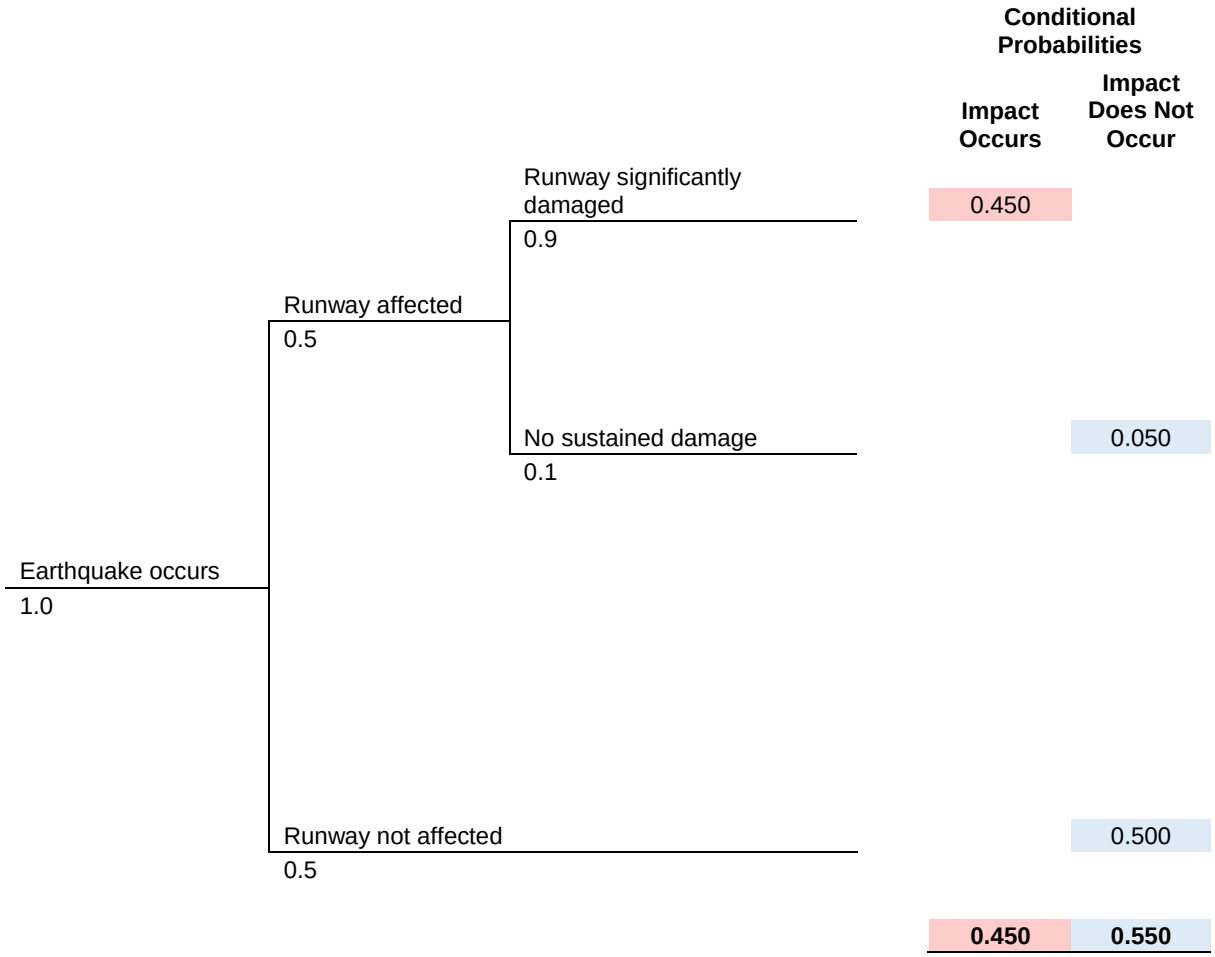


Figure E-2. Example Event Tree: Earthquake – Runway



Having identified consequence, threat probability, and asset vulnerabilities, risk for asset-natural hazard combinations can be calculated.

E5 – Natural Hazard Risk Mitigation

Upon determining and prioritizing risk for various asset-natural hazards combinations, mitigation measures can be identified. Many of the codes, standards, and guides described in Section 5, Security Mitigation Action Planning, are relevant in defining hardening measures for natural hazards. An example of natural hazard mitigation measures for earthquakes and tornadoes is provided below.

Options provided below were identified for assets relative to tornado and earthquake scenarios. A study should be performed to determine costs for upgrade or replacement of critical buildings using recommended building codes and options to protect non-building assets.

- Conduct Construction Standard and Building Upgrade/Replacement Study for critical buildings identified in the risk assessment that are subject to tornado threats. The study should determine current building standards for wind and earthquake magnitude and cost to upgrade/replace buildings to recommended standards (148 mile per hour [mph] winds [Enhanced Fujita [EF] 3 tornado] and seismic accelerations of Ss = 0.353 g and S1 = 0.076 g). Operational asset construction would also include 150 mph, Penetrating Type, Schedule 40 pipe.
- Build future critical buildings to recommended standards.

TORNADO DESIGN

Four documents are relevant when assessing tornado design:

- Department of Energy (DOE) Standard 1020 – Natural Phenomena Hazards Analysis and Design Criteria for DOE Facilities
- American Nuclear Society – ANSI/ANS-2.3-2011 – Estimating Tornado, Hurricane, and Extreme Straight-Line Wind Characteristics at Nuclear Facility Sites
- Development of a Probabilistic Tornado Wind Hazard Model for the Continental U.S., Volume 1, Lawrence Livermore National Laboratory, US Department of Energy, July 2000
- Tornado Climatology of the Contiguous U.S., Pacific Northwest National Laboratory, February 2007

These documents address the 3-second design wind speeds for various intensity tornadoes based upon the EF Scale and the size and velocity of potential wind-borne missiles. Though intended for nuclear facilities, these criteria can be applied to a facility that warrants an increased level of wind resistance. Where the risk of tornado damage exceeds acceptable risk, the recommended level of design is DOE Wind Design Category 3, which includes tornado criteria. The 3-second wind speed and the probability of exceedance are listed below:

Table E-4. 3-Second Wind Speeds and Probability of Exceedance

Probability of Exceedance	Lawrence Livermore National Laboratory	Pacific Northwest National Laboratory
0.001 (1:1,000)	NA	110 mph (EF 1)
0.0001 (1:10,000)	NA	148 mph (EF 3)
0.00001 (1:100,000)	156 mph (EF 3)	186 mph (EF 4)
0.000001 (1:1,000,000)	191 mph (EF 4)	222 mph (EF 5)

It should be noted that the Pacific Northwest National Laboratory analysis yields wind speeds somewhat greater than the methodology employed in the Lawrence Livermore Laboratory analysis. Given the uncertainty in determining the wind speed, it is conservative to use the Pacific Northwest National Laboratory values in design.

For missile size and velocity, it is recommended that criteria in ASCE 7-10[52] for wind-borne debris regions for the appropriate occupancy category be incorporated into the design for the glazing. Those provisions are outlined in Section 26.10.3 of ASCE 7-10. The ANSI document contains examples of missiles that can potentially damage the exterior cladding, including automobile contact, penetrating piping missile, or a solid steel sphere. Inclusion of the larger, more damaging missiles could be implemented on a case-by-case basis, given the type of building under consideration.

BUILDING SEISMIC DESIGN

ASCE 7 and the International Building Code only address life safety for the minimum design loads. Performance-based design criteria for seismic design are currently available for rehabilitation of existing buildings, but have not yet found their way into new building design. ASCE 41-06, Seismic Rehabilitation of Existing Buildings outlines the design criteria for earthquakes, and allows for

[52] ASCE 7, Minimum Design Loads and Associated Criteria for Buildings and Other Structures, American Society of Civil Engineers.

performance-based design based on the facility. The building performance levels and anticipated level of performance are summarized in Table E-5.

Once a Target Building Performance Level has been selected, specific Structural Performance Levels for both the main structural system and the non-structural components are selected to provide the Target Building Performance Level.

Table E-5. Summary of Building Performance Level

Target Building Performance	Overall Anticipated Damage
Collapse Prevention	Severe
Life Safety	Moderate
Immediate Occupancy	Light
Operational Level	Very Light

Though intended for building rehabilitation, the provision could be applied at levels above life-safety for new building construction for facilities requiring immediate occupancy or an operational level of performance. Application of the criteria would then be applied per the ASCE 41-06 requirements.

It should be noted that in the future, seismic design provisions will tend more towards performance-based design, rather than life-safety alone, to better align the design criteria with the intended performance of the facility. FEMA is engaged in developing new performance-based seismic design criteria, and it is anticipated those criteria will be adopted in future codes.

This example highlights the importance of including SMEs in assessing and implementing countermeasures and mitigation projects.

APPENDIX F: BENEFIT/COST ANALYSIS DATA SOURCES

Data that is useful in performing Benefit/Cost Analysis (BCA) is provided in tables F-1–F-4, below. All values are derived from FEMA guidance and have been adjusted to 2019 values.

Table F-1. Project Useful Life Estimates

Project Type	Useful Life (years)		Notes
	Standard Value	Acceptable Limits	
Acquisition/Relocation			
All Structures	100	100	
Structural/Non-Structural Building Projects			
Public Building Retrofit	50	50–100	
Historic Building Retrofit	50	50–100	
Roof Diaphragm Retrofit	30	30	Roof hardening and roof clips
Safe Room	30	30	
Non-Structural Building Elements	30	30	Ceilings, electrical cabinets, generators
Non-Structural Major Equipment	15	15–30	Elevators, HVAC, sprinklers
Non-Structural Minor Equipment	5	5–20	Generic contents, racks, shelves
Ignition-Resistant Construction	10	10–30	Depends on construction type/materials
Infrastructure Projects			
Major Infrastructure	50	35–100	
Concrete Infrastructure	50	35–50	
Equipment Such as Generators	5	5–30	
Utility Mitigation Projects	50	50–100	Major (power lines, cable, hardening gas, water, sewer lines)
	5	5–30	Minor (backflow values, downspout disconnect)
Miscellaneous Equipment Projects			
Equipment Purchases	10	2–10	Small, portable equipment (computers)
	30	5–30	Heavy equipment

Table F-2. FEMA Standard Values

Data Type	Value
Discount Rate	7%
Building Damage (percentage) that would Result in Demolition	Non-Historic Buildings: 50% Historical Buildings: 50% to 90%
Contents Value	50%-100% of the total building replacement value depending on building use.
Displacement Costs (2019)	$1.76/square foot/month

Table F-3. Dollar Values for Avoided Casualties

Injury Severity Level	Value
Fatality	$9,486,106
General Average for Injuries	$649,281
Hospitalized	$1,322,481
Treat & Release	$109,396
Self-Treatment	$14,586

Table F-4. Standard Displacement Costs for Various Building Types

Building Type	Rental Cost (2019) $/ft^2/month	Disruption Costs (2019) $/ft^2
Commercial		
Retail Trade	1.52	1.42
Wholesale Trade	0.63	1.24
Professional/Technical/Business	1.77	1.24
Banks	2.21	1.24
Medical Office/ Clinic	1.77	1.77
Entertainment and Recreation	2.21	0.00
Parking	0.44	0.00
Industrial		
Heavy	0.26	0.00
Light	0.35	1.24
Food/Drugs/Chemicals	0.35	1.24
Metals/Mineral Processing	0.26	1.24
High Technology	0.44	1.24
Construction	0.18	1.24
Government		
General Services	1.77	1.24
Emergency Response	1.77	1.24

APPENDIX G: AIRPORT SECURITY VULNERABILITY ASSESSMENT REPORT TEMPLATE

A recommended SVA report template is provided below. Instructional language is provided in *italics* throughout the template.

Handling Instructions

Handling instructions should be included if sensitive security information is contained in the SVA Report.

The information, records, meetings, analysis, and report information contained in this document were generated as a result of the comprehensive Security Vulnerability Assessment (SVA) and are considered Sensitive Security Information and exempt from applicable laws and rules requiring public access and disclosure.

Executive Summary

Provide Executive Summary highlighting high-risk asset-threat combinations and mitigation recommendations.

1. Introduction

Overview

State purpose for the SVA from the Project Charter.

Project Charter

Summarize information in the project charter regarding SVA focus, goals, objectives, and team members.

Methodology

Describe the steps used to conduct the SVA.

Step 1: Project Charter

Step 2: Asset Characterization

Step 3: Threat Characterization

Step 4: Consequence Analysis

Step 5: Probability Analysis

Step 6: Vulnerability Analysis

Step 7: Risk Calculation and Risk Ranking Methodology

Step 8: Risk Management

2. Asset Characterization

Overview

The overall purpose of asset characterization is to determine the assets that, if compromised by a threat, could result in interruption of service, functional degradation, injuries, fatalities, detrimental economic impact, or any combination thereof.

Airport Mission

Describe mission and potential impacts based on assets being compromised.

Potentially Critical Assets

Describe assets that may impact mission if compromised.

Protective Countermeasures/Mitigation Measures

Describe existing mitigation/countermeasures that may reduce asset vulnerability to specific threats.

Worse Reasonable-Case Consequences

Describe worst-case scenarios that may be expected if assets are compromised by specific threats.

Prioritized Critical Assets

Based on worst reasonable-case consequences, prioritize assets for further assessment.

3. Threat Characterization

Overview

Threat characterization identifies relevant threat scenarios to be considered. A threat is an event with negative consequences carried out through malicious human intent. Upon conclusion of this step:

1. A list of malevolent threats will be identified and those threats that have a reasonable likelihood of occurrence will be addressed in consequence analysis.
2. Threats will be addressed relative to critical assets identified in Asset Characterization and their relevance to each critical asset will be ranked based on a broad estimation of potential impact (high, medium, or low).
3. Critical assets linked to specific threats will be identified to facilitate cross-asset comparison of risk. Threat characterization ultimately seeks to identify relevant asset-threat combinations to

assess in the remainder of the SVA process (i.e. those asset-threat combinations with a medium or high estimation of potential impact).

Potential Malevolent Attacks

Describe reference threats (add or remove threats as necessary):

1. Armed Attack – Attack by one or more persons using firearms or other weapons;
2. Arson – Deliberately setting fire to property;
3. Assault – Physical or verbal attack on one or more persons involving patrons and/or employees;
4. Attack: Explosives <=5 kg TNT Equivalent – An attack using an explosive or improvised explosive device (IED) such as a package or pipe bomb, mail/courier delivered package, or possibly drone-dropped;
5. Attack: Explosives <=15 kg TNT Equivalent – An attack using an explosive or improvised explosive device (IED) such as a backpack or luggage bomb;
6. Attack: Explosives <=500 kg TNT Equivalent, Small VBIED – An attack using a small vehicle-borne improvised explosive device (VBIED) to deliver to target such as a passenger car;
7. Attack: Explosives >=500 kg TNT Equivalent, Large VBIED – An attack using a large vehicle-borne improvised explosive device to deliver to target such as a van or truck.
8. Attack: Release of Infectious Agents: An attack releasing biological, chemical, or radiological agents in public areas.
9. Civil Disorder/Protest – Disturbance of the public peace by multiple persons, generally in public areas such as roadways or terminals, which may impact operations;
10. Sabotage – Deliberately destroying damaging, or obstructing property in such a way as to render it inoperable, generally for economic or political reasons;
11. Theft – To steal property within the airport, generally for personal gain;
12. Trespassing – To enter secured areas without permission or consent;
13. Vandalism – Deliberate malicious act to damage or destroy property; and
14. Vehicle as a Weapon – An attack (not involving explosives) using a vehicle to inflict damage on people, property, or operations.

Asset-Threat Combinations

Match assets with relevant threats which may result in operational degradation/interruption.

Critical Asset-Threat Combinations

Use worst-reasonable case scenarios to identify critical asset-threat combinations. Either due to existing countermeasures or other conditions, some assets may not be susceptible to specific threats.

4. Consequence Analsyis

Overview

Consequence analysis is performed to estimate potential losses from the exposure of threats to specific assets. Consequences are assessed based on five primary components as indicated in Table X.

Table X. Components of Consequence Analysis for Airport SVAs

Component	Description
Number of Fatalities	Estimate of the number of fatalities anticipated for a specific asset-threat combination.
Number of Injuries	Estimate of the number of injuries anticipated for a specific asset-threat combination.
Displacement/Workaround Costs	Estimate of the cost of temporary displacement and/or workaround costs necessary to sustain operations.
Replacement/Repair Costs	Estimate of the cost of repair or replacement cost for assets damaged due to a specific threat.
Loss of Service Costs	Estimate of the loss of service costs associated with any downtime or reduced service potential due to a specific threat.

Worst Reasonable Case Application

To the extent possible, quantify the worst-reasonable case for each asset-threat combination.

Consequences for Asset-Threat Combinations

Describe consequences for each asset-threat combination in terms of the five components in the Table above.

5. Probability Analysis

Probability analysis is the estimate of the likelihood of each specific threat occurring and is generally based on intelligence or historical data as well as estimates of the asset's attractiveness to the perpetrator and the ease with which the threat can occur. Probability is a measure of the likelihood, degree of belief, frequency, or chance that a particular event will occur in a defined period (usually one year).

For malevolent threats, the relative attractiveness of the specific target is based on evaluation of alternative targets and probability of success.

Use proxy measures provided in Guidance, local statistics, and/or subject matter experts to estimate probability of threats.

6. Vulnerability Analysis

Overview

Vulnerability serves as a measure of the organizational, physical, and technical conditions that can be exploited by a perpetrator to improve the probability of success of committing a malevolent act. Conditions that determine the level of vulnerability of a given asset to a specific threat may include:

- Asset characteristics – Building/construction standards, level of physical security, and equipment characteristics;
- Technology – Systems available to deter, detect, and defend against threats; and
- Operational Practices – Plans, policies, and procedures, training and quality assurance, and personnel practices.

Facility Construction, Systems, and Layout

Document actions taken to identify vulnerabilities. Tasks to support vulnerability analysis include:

1. Review and document pertinent asset, equipment, and technology specifications and facility layout;
2. Identify countermeasures, mitigation measures, and other impediments to threats that provide deterrence, detection, or delay capabilities;
3. Assess local supporting operational response measures; and
4. Identify processes within the airport that impact threat potential.

Vulnerabilities of Critical Assets

Establish vulnerabilities using event trees which assess the general pathways for malevolent threats to occur and relative probabilities.

Document specific assets and associated vulnerabilities.

7. Risk Analysis

Risk Calculation

Risk is calculated for each asset-threat combination using the equation:

Risk = Consequence x Vulnerability x Threat Likelihood

Summarize risk in table and/or narrative format.

Risk Ranking

Provide a risk ranking as an initial step in prioritizing risk mitigation needs.

8. Risk Management

Potential Countermeasures and Mitigation Options

Summarize countermeasures and mitigation options that may reduce risk among prioritized asset-threat combinations.

Assessment of Countermeasures and Mitigation Options

Efficacy of Options

Assess and summarize the efficacy of various countermeasures and mitigation options in reducing risk among prioritized asset-threat combinations.

Benefit/Cost Analysis

Assess benefits and costs to identify benefit/cost ratios.

Assessment Results

Prioritize recommended mitigation measures using benefit/cost ratios.

Security Mitigation Action Plan

Roles and Assignments

Define roles and assignments in developing specifications, procuring, and implementing various countermeasures and mitigation options.

Procurement Needs

Define procurement needs including budget, engineering support, design, and other parameters.

Schedule/Timeline

Develop a schedule and milestones to manage project implementation.

Appendix A – Asset Descriptions

Provide brief (1-page) descriptions of assets with pictures as desired.

Appendix B – Consequence Analysis Data

For each asset-threat combination, document calculations for: 1) Number of Fatalities; 2) Number of Injuries; 3) Displacement/Workaround Costs; 4) Replacement/Repair Costs; and 5) Loss of Service Costs.

Appendix C – Probability Assessment Data

For each asset-threat combination (or groups of asset-threat combinations), document probability assessment and considerations in determining probabilities.

Appendix D – Vulnerability Assessment Data

For each asset-threat combination (or groups of asset-threat combinations), document vulnerability using event trees or other desired method (such as qualitative analysis).

Appendix E – Security Mitigation Action Plan

For each asset-threat combination which exceeds acceptable risk levels, provide a mitigation action plan (in tabular or narrative format) which documents the following information for each mitigation options chosen:

1. Efficacy of Options
2. Benefit/Cost Ratio (BCR)
3. Roles and Assignments
4. Procurement Needs
5. Schedule/Timeline

Tabular example provided below. Action plan should be used to track progress.

Table X. Components of Consequence Analysis for Airport SVAs

No.	Mitigation Measure	Efficacy	BCR	Assignee	Procurement Needs	Desired Deadline
1						
2						
3						