PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0011 January 2019

Guidance for Airport Security Master Planning

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Faith Group, LLC
St. Louis, MO

COPYRIGHT INFORMATION

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 airport security technology and procedures.

Through the Airport Security System Integrated Support Testing (ASSIST) 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 Performance and Operational System Testing (POST) Program, Safe Skies assesses the continued operational effectiveness of airport-owned security technologies.

Through the Program for Applied Research in Airport Security (PARAS), 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 for 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 Special Programs Manager*

PARAS 0011 PROJECT PANEL

Frank Capello *Broward County Aviation Department*
Sean Cusson *LAM-LHA USA, LLC*
Sarah Demory *Phoenix Sky Harbor International Airport*
Mark Inzana *Denver International Airport*
Scott Lanter *Blue Grass Airport*
Dawn Lucini *Telos Identity Management Solutions*
Bill Marrison *McGhee Tyson Airport*
Bill McAteer *McAteer and Associates Consulting*
Melissa Osborn *Fairbanks International Airport*

AUTHOR ACKNOWLEDGMENTS

Faith Group would like to acknowledge the following for their contributions in the development of this guidebook:

- National Safe Skies Alliance's PARAS, which provided funding. Thanks are given to the program manager, Jessica Grizzle.
- The PARAS 0011 Project Panel Members, who also provided significant review and contributions.
- The airports who provided invaluable input during use case interviews and surveys to vet the draft Guidebook sections; the direction of this guidebook was shaped, in part, thanks to their input:
    - Baltimore-Washington International Airport
    - Bethel Airport
    - Clinton National Airport
    - Denver International Airport
    - Fairbanks International Airport
    - General Mitchell International Airport
    - Kansas City International Airport
    - Lincoln Airport
    - Memphis International Airport
    - Oakland International Airport
    - Orlando International Airport
    - Philadelphia International Airport
    - Port Authority of New York/New Jersey (five airports)
    - Raleigh-Durham International Airport
    - Sacramento International Airport
    - San Antonio International Airport
    - San Francisco International Airport
    - San Jose International Airport
    - Spokane International Airport
    - St. Louis Lambert International Airport
- The team of authors from the following firms who contributed to this document:
    - Faith Group, LLC, Principal Investigator
    - The JW Group (JWG)
    - Booz Allen Hamilton

CONTENTS

LIST OF TABLES & FIGURES

SUMMARY

This guidebook is intended to be used by airport management and staff, as well as security consulting organizations as a holistic approach to developing and implementing a Security Master Plan (SMP). An SMP enables an airport to systematically support the forecasting and planning of future security needs and the associated capital expenditures. Expenditures at a minimum may include security technology solutions and infrastructure to support security standards. Other benefits for security stakeholders may include improved policies and procedures for operational departments responsible for implementing and maintaining security infrastructure.

An SMP is not intended to replace or duplicate the Airport Security Program (ASP), which is mandated by the DHS under TSA 49 CFR § 1542. Future needs planning and security project development requires a separate undertaking. The guidebook approaches an SMP effort as its own project with a management team, charter, and clear objectives supported by goals. As with any project, an airport's security organization needs to understand what it intends to accomplish and identify the timing and method for funding.

The reader will be able to follow the guidebook section by section or utilize independent sections, depending on the airport's objectives. The guidebook is intended to offer different approaches and tools for all sizes of airports. Once an SMP is established, it should be systematically updated and refreshed regularly to ensure validity and relevance.

PARAS ACRONYMS AND ABBREVIATIONS

The following acronyms and abbreviations are used without definitions in PARAS publications:

ACRP	Airport Cooperative Research Project
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue and Fire Fighting
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
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

SECTION 1: OVERVIEW OF GUIDEBOOK

Section 2: Introduction and Purpose explains the principles of developing and maintaining an SMP, and its usefulness to airport management and staff.

Section 3: SMP Process guides the reader through each step of the project process.

Section 4: Scoping and Strategy Phase guides the reader through facilitating the process with sample project management tools. As with any other project at the airport, the SMP is a planning process. In order to be successful, it needs a foundation and a good team with a project manager. This section helps the project team organize and manage their processes.

Section 5: Existing Conditions Phase is a critical step for any airport SMP process. This section guides the reader in gathering existing conditions data and explains how to balance that information with future goals. This section should be utilized when beginning SMP projects and for future gap analysis to continuously measure where airports are and where they want to be. It is part of the continuous improvement process.

Section 6: Functional Areas and Technology follows on from the existing conditions phase with a deeper dive into understanding what the airport has and what it needs, including addressing critical infrastructure to meet the airport's goals. This is an especially important section since technology is becoming an impactful driver for most airports; however, technology solutions are not always the only or best solution for every airport, especially for small airports constrained by funding sources.

Section 7: Development and Action Phase guides the reader towards implementation of the SMP and the final steps to conduct gap analysis studies for all aspects of security at the airport including a threat and vulnerability analysis. This will support the airport roadmap and implementation of the SMP.

Section 8: Monitoring and Maintenance Phase guides the reader on how to maintain the planning process. It is a continuous process of changes, adaptations, and improvements. An SMP, just as any other airport program, is a living, breathing, and adapting process.

Section 9: Conclusion is a summary of key takeaways the guidebook delivers, and reinforces the positive aspects of developing and maintaining an SMP.

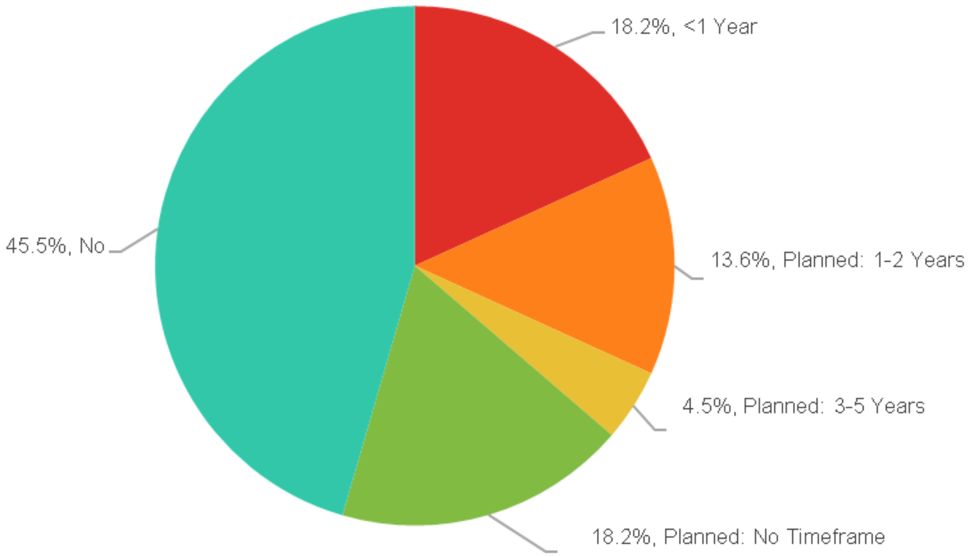
SECTION 2: INTRODUCTION AND PURPOSE

In this section, the reader will gain an understanding of why an SMP is needed and how to integrate it into the Airport Master Plan (AMP) for long-term goals that support efficient and effective daily airport security operations.

Security departments or organizations at airports have historically focused their efforts on maintaining compliance with their ASPs, areas where there are perceived and/or known vulnerabilities, known threats, or responding to Security Directives from TSA, and issues or events that had occurred in the past. The ASP, as a regulatory document, does not provide for planning guidance from a holistic airport security perspective. It typically details the airport's commitments to the regulations but cannot be the sole source for achieving a progressive and comprehensive security program. Additionally, tactical and/or reactive responses to issues and events, however valid, should also not be the primary driver of airport security decision-making.

An SMP is an excellent way to improve an airport's overall safety and security posture, tying in the operational and planning aspects across all the airport functional areas. Creating this type of planning document enables the security department to work with airport leadership to be better prepared to implement and fund an aviation security program providing the level of informed pre-planning, control, and situational awareness necessary to be proactive in mitigating risks, as well as intelligently and efficiently respond to incidents. As a first step into the topical areas of an SMP, an example table of contents has been provided as Appendix A to this guidebook. This table of contents was vetted by surveying airports as to content relevance and interest in creating an SMP. Figure 1 shows the breakdown of responses when airports were asked about their plans for developing an SMP.

Figure 1. Airport Plans to Develop and SMP (22 total responses)



An SMP provides a basis for security planning associated with rules, regulations, processes, people, and technology at an airport. The questions that must be asked are:

- Is your airport basing the design and implementation of your security measures—including technology—on a well-planned vision and strategy, or are all security initiatives tactical in nature or specific to meeting compliance in the ASP?

- Is this strategic vision endorsed by leadership and management?
- Are the overall goals, objectives, and approaches sufficiently documented?

It is critical that the reader has a basic and common definition of an SMP. An SMP is not only a security assessment, although it includes a comprehensive process for evaluating security-related improvement opportunities. An airport SMP is a business plan for the airport security department, providing a vision of the many airport departments and group roles and responsibilities, and how security fits into the overall organization. Airport leadership and management must endorse it, making it an enterprise-wide framework that provides a big-picture context for all security measures, planned improvements, and coordination amongst airport departments and agencies.

An example definition of an SMP is expressed below (Giles 2008).

> *A Security Master Plan is a document that delineates the organization's security philosophies, strategies, goals, programs, and processes. It is used to guide the organization's development and direction in these areas in a manner that is consistent with the company's overall business plan. It also provides a detailed outline of risks and the mitigation plans for them in a way that creates a five-year business plan.*

There are many steps in the development of an SMP based on a basic framework, which includes existing conditions, gap analysis, risk analysis/management, and recommendations (Figure 2). The specific form it takes hinges on the current condition of the airport, its ASP, and the processes that are in place and operational. Each airport is unique, and the SMP must be customized to fit the needs, concerns, and expectations of its specific constituents and stakeholders. The SMP, from the outset, should be considered a living document interfacing with and supporting the AMP, IT Master Plan, and any other operational Master Plans. The information contained in the SMP should be subject to constant review in the light of changing requirements and regulations.

Figure 2. SMP Content

Security Master Plan
• Existing Conditions
• Gap Analysis/Risk Assessment
• Recommendations

To develop an effective SMP, it is critical to document the airport security department's mission and objectives, in addition to equipment, policies, procedures, and technology to be used in securing and monitoring the facility. Benchmarking of similar airports against these basic attributes will help assess current conditions.

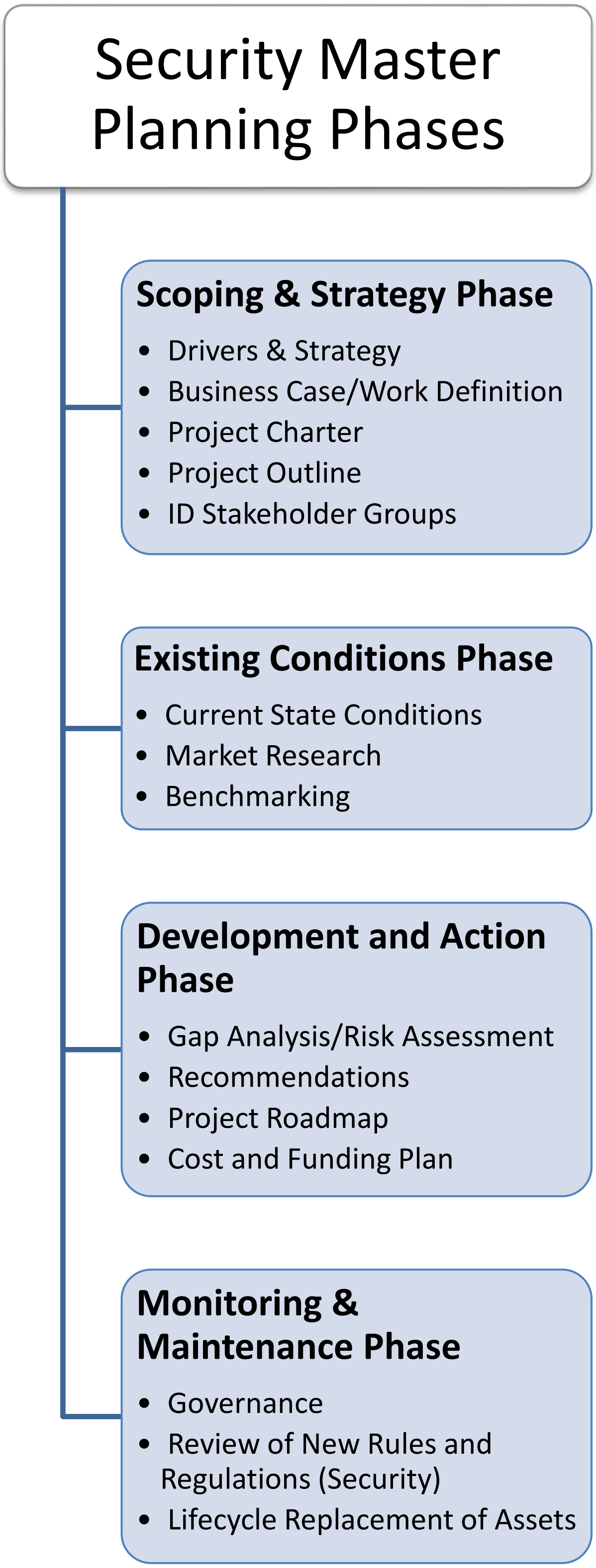
The intent of an airport SMP is to provide the airport with a framework of guidelines for the selection, implementation, management, and operation of programmatic, procedural, physical, electronic, environmental, and behavioral security modifications designed to minimize risk and maximize the protection of the airport’s passengers, employees, property, and information, while maintaining regulatory compliance.

It is further the intent of the SMP to define or recommend a project to create the airport’s standards for the security systems, boundaries, hardware and software, and policies and procedures to be utilized in and around new and existing facilities. Examples of security systems may include technology-based systems such as the Access Control and Alarm Management System, Video Surveillance System (VSS), Perimeter Intrusion Detection System (PIDS), and Security Communication System, and may often include low-tech systems such as boundary fence standards, or policies and procedures associated with vendor and employee inspections and tenant facility modification reviews.

The airport SMP uses threat and vulnerability assessments as well as a gap analysis process (see Section 7) as a foundation for developing guidelines and supporting a solid Business Case for infrastructure process and procedures changes and/or enhancements. An SMP must also evaluate and incorporate previous assessments of threats faced by the airport. All assessments that may have been undertaken, including those led by the airport, TSA, FBI or other law enforcement agencies, should be considered and incorporated into the planning process. The Vulnerability/Risk Analysis along with the assembled benchmarking data is further used to help define the priorities for a set of risk mitigation recommendations. This is the foundation of a security Business Case.

SECTION 3: THE SECURITY MASTER PLANNING PROCESS

Figure 3. Security Master Planning Phases



Security Master Planning Phases

Scoping & Strategy Phase

- Drivers & Strategy
- Business Case/Work Definition
- Project Charter
- Project Outline
- ID Stakeholder Groups

Existing Conditions Phase

- Current State Conditions
- Market Research
- Benchmarking

Development and Action Phase

- Gap Analysis/Risk Assessment
- Recommendations
- Project Roadmap
- Cost and Funding Plan

Monitoring & Maintenance Phase

- Governance
- Review of New Rules and Regulations (Security)
- Lifecycle Replacement of Assets

The SMP process is a linear and sequential approach to developing the plan. Each phase in the process builds upon the next, resulting in clear and concise recommendations that should align with the organization's security goals and objectives. Typically, the SMP process has four distinct phases, as identified in Figure 3. An SMP should begin with a Strategy Phase that defines the drivers for the plan, establishes the Business Case and justification, and reviews and aligns the airport's security department or organization's objectives and security goals. The plan should conclude with the Monitoring and Maintenance phase, which establishes the strategy for the continued review of the plan's implemented recommendations, future proposed recommendations, review of new regulations and the ongoing asset replacement to keep it up-to-date and dynamic. Airports need to view the SMP as a living, changing, strategy blueprint that assists the airport in meeting security compliance and planning security needs.

3.1 Introduction

The SMP process involves many different moving parts, including precursors such as utilizing a Project Management Plan to define a Business Case, Project Charter, and overall project plan. There are many Project Management Plan processes and personnel certification programs available. Figure 3 provides the steps and potential activities in each step to define an SMP scope, including key planning tools, resources, drivers, and strategies, as well as the risks of not having an SMP.

3.2 Scoping and Strategy Phase

During the scoping and strategy phase, the SMP process will include development of a Business Case, Project Charter, and project outline, and identification of stakeholders from the airport (e.g., key staff, tenants, and external groups).

3.3 Existing Conditions Phase

The existing conditions phase will consist of documenting the current state and condition of security-related items such as systems, networks, staffing, policies, and procedures. Market research on industry standard and trending technologies will be developed, and benchmarking against airports will occur.

3.4 Development and Action Phase

The development and action phase assesses the current state by identifying gaps or needs and performing a risk assessment to determine the best course of action for adding, updating, or replacing security-related items. Recommendations will be developed, and a project road map will be created with rough order of magnitude (ROM) costing and associated spending plan, so that a phased-approach to funding can be established through the airport's capital improvement process.

3.5 Monitoring and Maintenance Phase

During the monitoring and maintenance phase, a plan for governance, periodic review of systems, policies and procedures, new rules and regulations (as they pertain to securing the airport's assets), and a lifecycle replacement program should be initiated.

SECTION 4: SCOPING AND STRATEGY PHASE

4.1 Drivers and Strategy

Motivations for airport security to develop an SMP can range from controlling costs associated with the purchase, installation, maintenance, and upgrades of security system components to a calculated response to breaches or security incidents.

Airports surveyed in 2018 also mentioned other motivating factors associated with their desire to have an SMP, including planning for the following:

- Capital funding needs
- Infrastructure support
- Space/land use
- Mitigation of threats and vulnerabilities
- Future staffing needs
- Project management office
- Tenant security standards
- Public area security
- Cyber and emergency management

Developing an SMP can also be part of a larger airport strategic objective:

- Executive buy-in (Strategy)
  - Quick glance report/Business Case
  - Critical success factors
  - Costing and funding
- Existing conditions (Driver)
- Design constraints (Strategy)
- Technology factors (Driver/Strategy)
- Passenger experience (Driver/Strategy)
- Risks of not having an SMP (Driver)

Key drivers mentioned for a non-hub airport surveyed included:

- Weakest area is in security planning
- Security is not viewed as important
- The airport needs to articulate the value
- A statement of services should be included in the Master Planning process
- A state-wide standard set of criteria and approach to security is needed

4.2 Business Case and Project Charter

A Business Case is a precursor document (deliverable) to the Project Charter to begin work on an SMP.

The use of a Business Case is considered standard practice throughout the industry and in today's cost- and metrics-focused airport business environment, airport security practitioners must be able to understand and apply the process.

A well-written Business Case provides compelling justification for initiating the SMP. It is often presented in a formal structured document. The premise of the Business Case is that whenever airports request resources, those resources should be in support of a specific, well-defined need.

Depending upon the internal working rules for a department or organization at an airport, the value of an SMP may need to be researched, documented, and justified prior to being approved. The assumption is that a Business Case resolves the questions pertaining to a problem (i.e., benefit analysis or cost/benefit analysis), and in this case, the problem would be a lack of planning for the future of security-based systems and initiatives.

The results of the SMP will be a set of project recommendations, as seen in Section 7.4. It can reasonably be expected that the security professional presenting SMP recommendations and the associated proposed yearly budget plan to airport management will also be responsible for providing a Business Case to justify the proposed recommended projects. To support this effort, a recommendation template (Table 8, Section 7.4) has been provided to document each recommended project.

A Project Charter is defined as a document that provides the main purpose or intended goal, identifies stakeholders, and delineates roles and responsibilities, including the lead project manager as the reference of authority. The charter is used by the airport as the guideline for starting the SMP process.

Best Practice: If the airport does not follow a formal Business Case process (e.g., small-hub airport), a Project Charter should still be used as the defining document for the creation of an SMP.

Development of a Business Case can be started with answering the following questions at a minimum, and should be tailored to an individual airport's needs:

1. What is the status of aviation security at the airport in terms of the systems, operations, processes, procedures, technologies, capabilities, staffing, and ongoing work?

2. What is the future of aviation security, based on national, international, and local issues, including changes in technologies, regulatory requirements, airport growth, and operations?

3. What is the current state-of-the-art and best practices for aviation security at similar airports?

4. How does the current state of aviation security at the airport compare to aviation security at peer airports and the potential future aviation security outlook? Are there gaps, weaknesses, and vulnerabilities at the airport? Are the existing aviation security technology systems at or near end-of-life?

5. What is and what should the aviation security philosophy and strategy be at the airport?

For an airport to move forward with an SMP, it should create a Business Case that is simple and to the point to provide executives and management with the necessary information to move the project forward in the approval process. A useful resource for airport security professionals is the *Security Business Case*

Development Guide published by ASIS. A high-level outline of the Business Case sections is provided below; Appendix B contains more details in the Business Case Example:

1. Introduction – Describes the purpose of the Business Case
2. General Project Information – Includes a description of the business need, goals of an SMP, and scope
3. High Level Business Impact – Describes the impact on the business for developing and implementing the SMP
4. Alternatives and Analysis – Identifies the options and alternatives in developing the SMP, considering strategy, approach, limitations, funding, and scheduling
5. Preferred Solution – Develops the recommendation for the SMP based on the alternatives, including costs, schedule, and procurement options, and documents any assumptions or constraints

Because preparation of an SMP is a team effort, a listing of the recommended stakeholders is explored in the next subsection. These high-level questions require a significant effort for the team to define and analyze, with the results presented to executive management within the SMP. Ultimately, the information provides an understanding of the foundation from which any new security-related system, operation, process, procedure, and technology is to be developed and implemented.

However, it must be pointed out that in some areas of this process, it will be difficult for an internal person to be completely objective. Areas such as defining the current skills and knowledge of the security organization may be especially difficult. If an airport chooses to implement this process on their own, a best practice to consider is to supplement internal talents with others who may be more skilled in certain areas, or who might provide another approach. This type of integrated-team approach can be an effective way to achieve the best result for that airport.

Whether the airport's security department or organization elects to perform the SMP process in-house or contracts professional services, it is recommended that the team settle on a group of guiding principles. For this effort, the following ideas are proposed as the basis for any future security planning:

- Security systems must be designed to support and enhance security and operations, while remaining technically sound and easily adaptable to future requirements.
- Security systems must meet the goals of the airport and the stakeholder community, while respecting the realities of external requirements (e.g., security regulations) and limitations (budgets and funding).
- Solutions presented must embrace the idea of change and adaptation. As such, any solution and approach developed must remain flexible and adaptable, able to adjust to new requirements and situations without major changes to the systems themselves.
- Technology has become one of the single biggest driving factors in security design. It must be understood that any technology solution selected and deployed will drive costs, training, and the capabilities of the local security force and maintenance staff.
- Implementation of any new technology or the replacement of a system must not be driven solely by the fact that there is something newer available. In other words, change must be for the sake of improved security, not simply for the sake of change.

An example of a Business Case and Project Charter can be found in Appendix B.

4.3 Identifying Stakeholders

Stakeholders are identified in the project plan. Early input of stakeholder needs is critical in development of a comprehensive program. It is important that the SMP Team (SMPT) establish a list of key airport security stakeholders. Their viewpoints and suggestions must be considered in the early development of goals and objectives. Regardless of airport size, several of the following stakeholders may be included:

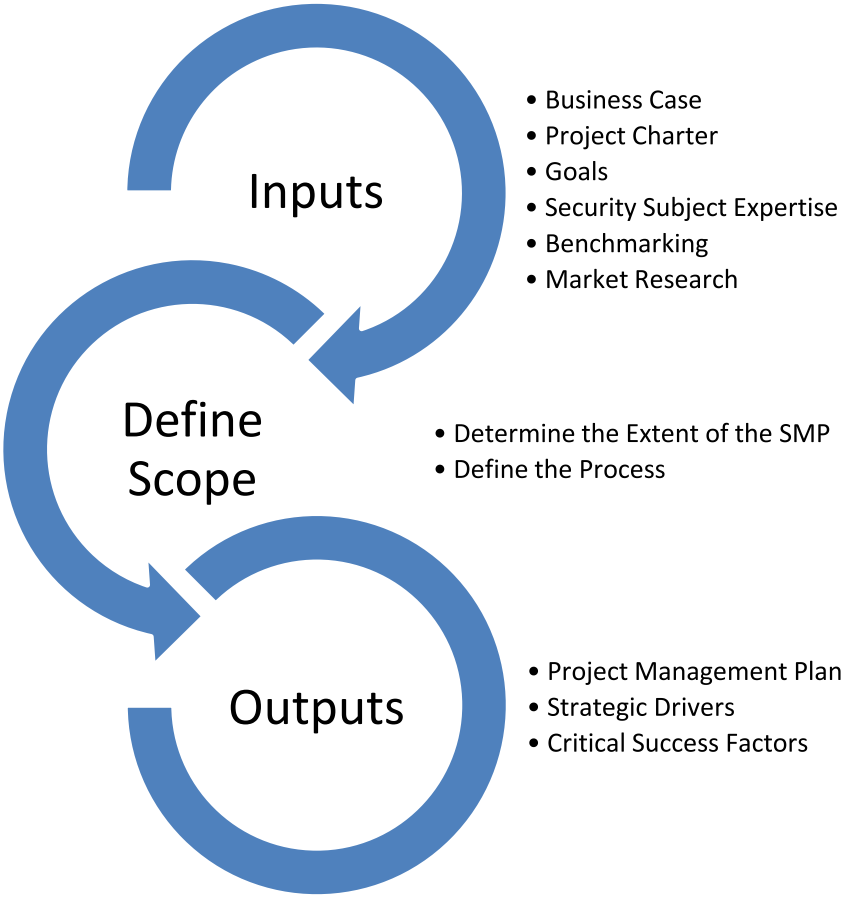
- Aircraft Catering
- Airport Adjacent Facilities
- Airport Security
- ARFF
- Business and Finance
- Cargo Airlines
- Communication Center/Dispatchers
- Customs and Border Protection (CBP)
- Emergency Management
- FBI
- Ground Handlers
- IT
- Law Enforcement
- Maintenance
- Operations (airside and landside)
- Passenger Airlines
- Planning and Engineering
- Private Security Contractors
- Terminal Food/Beverage/Concessions
- TSA

Subject-matter expertise should be considered when identifying key team members. If creating the team in-house, the airport security department should consider a person’s facilitation skills for determining who is best suited as the project lead. A project lead will need facilitation and project management skills and should be a security subject matter expert. Stakeholder department personnel who will be invited to participate and support this effort should include staff with decision-making capabilities or subject-matter experts. The airport SMP project lead should be employed and/or empowered by airport security department executive management and serve as a champion for the SMP. Utilizing staff for their skills also supports organization succession planning. Executive management should consider this approach for any new project start up. Involvement in a project such as an SMP allows employees to gain experience and exposure to multiple operating aspects of the airport environment, which may lead to potential succession opportunities.

4.4 Developing the Project Management Plan

A project scope is the part of project planning that is used to determine specific project goals, the order of tasks in which to accomplish the goals, and drivers and rules for the project team, including assignments, deadlines, and associated costs. A project scope not only addresses the project objectives, requirements, constraints, and assumptions, but it also is progressively updated as more planning details become known or are elaborated through the Project Management Plan scope statement. As an example, Figure 4 shows the inputs, tools, techniques, and outputs of the defined scope process.

Figure 4. Define Scope Process Example



The Project Management Plan is used to capture the Business Case, Project Charter, and Stakeholder list, as well as other management plans (e.g., communication plan, travel plan, etc.) A sample Project Management Plan is included in Appendix C.

Key planning tools help in the development of an SMP. Benchmarking and market research are tools commonly used to support the SMP, costing initiatives, and provide for industry best practices data. Benchmarking, as defined here, is the process of comparing an airport's security organization or program against other similar airports.

4.5 Understanding and Controlling SSI

Developing an SMP will require the SMPT to obtain as well as develop SSI. SSI is a control designation used by the DHS, and particularly the TSA. It is applied to information about security systems and programs, vulnerability and threat assessments, screening processes, technical specifications of certain screening equipment and objects used to test screening equipment, and equipment used for communicating security information relating to air or land transportation. The applicable information is spelled out in greater detail in TSA Regulation 49 CFR § 1520.

The SSI designation may apply to information the SMPT obtains or develops on its own while carrying out certain security or research and development activities associated with an airport SMP. SSI protects information that, if disclosed, could make it easier for hostile elements or bad actors to circumvent and/or avoid airport security controls.

The SMP project manager must lead the discussion for the use, handling, and control of SSI with the Airport Security Coordinator or designee. A best practice would be for the SMPT to use the airport security department or organization’s standard policies and procedures for the control and handling of SSI or create a policy specifically for the preparation of the SMP that follows the airport’s SSI policy. If possible, the SMPT should endeavor to develop the SMP in a way that allows for publishing the recommendations, costing, and roadmap sections of the document as non-SSI to allow for wider distribution.

The SSI Policies and Procedures should be included in the Project Management Plan. An example Model of an SSI Control Plan can be found in Appendix D.

SECTION 5: EXISTING CONDITIONS PHASE

5.1 Introduction

Using the objectives listed in the Scoping and Strategy Phase (Section 4) and guidance relative to the Development and Action Phase (Section 7), this section examines the process of documenting and assessing existing security-related conditions in such a way that the outputs identify risks, gaps, potential weaknesses and/or vulnerabilities, and areas that need attention.

Airports have in place a wide range of security plans, programs, policies, procedures, rules, regulations, and security systems, including but not limited to physical security boundaries and gates, electronic access control systems (ACS), ID badging systems, VSS, video management systems (VMS), and PIDS. These generally fall under the operational jurisdiction of either an airport security department or airport operations and communications centers.

This section will provide guidance on the best practices, standards, tools, and techniques to conduct an assessment and create the necessary documentation of the existing conditions and current state of security at the airport.

Gathering existing conditions for an airport SMP is an essential step in the process. For the SMPT to compare, evaluate, and recommend, it is essential that information is gathered in a way that represents the most accurate picture of the airport's actual and current security status. Equipment, systems, technologies, processes, and procedures across all facets of airport security must be understood and documented. By doing this, the SMPT learns about the airport and creates documentation that is used for reference during the next phases of the SMP process. Much of the information is gathered through stakeholder meetings, interviews, assessments, and existing documentation. An example of a table summary for existing conditions can be found in Appendix D .

The next step in the process provides information requiring a stakeholder validation review step. It is during this phase that the SMPT obtains detailed knowledge of the airport's physical layout, security systems, supporting technology, supporting infrastructure, processes, and policies. This knowledge is captured and serves as the guideline and reference material for the gap analysis and recommendations phases.

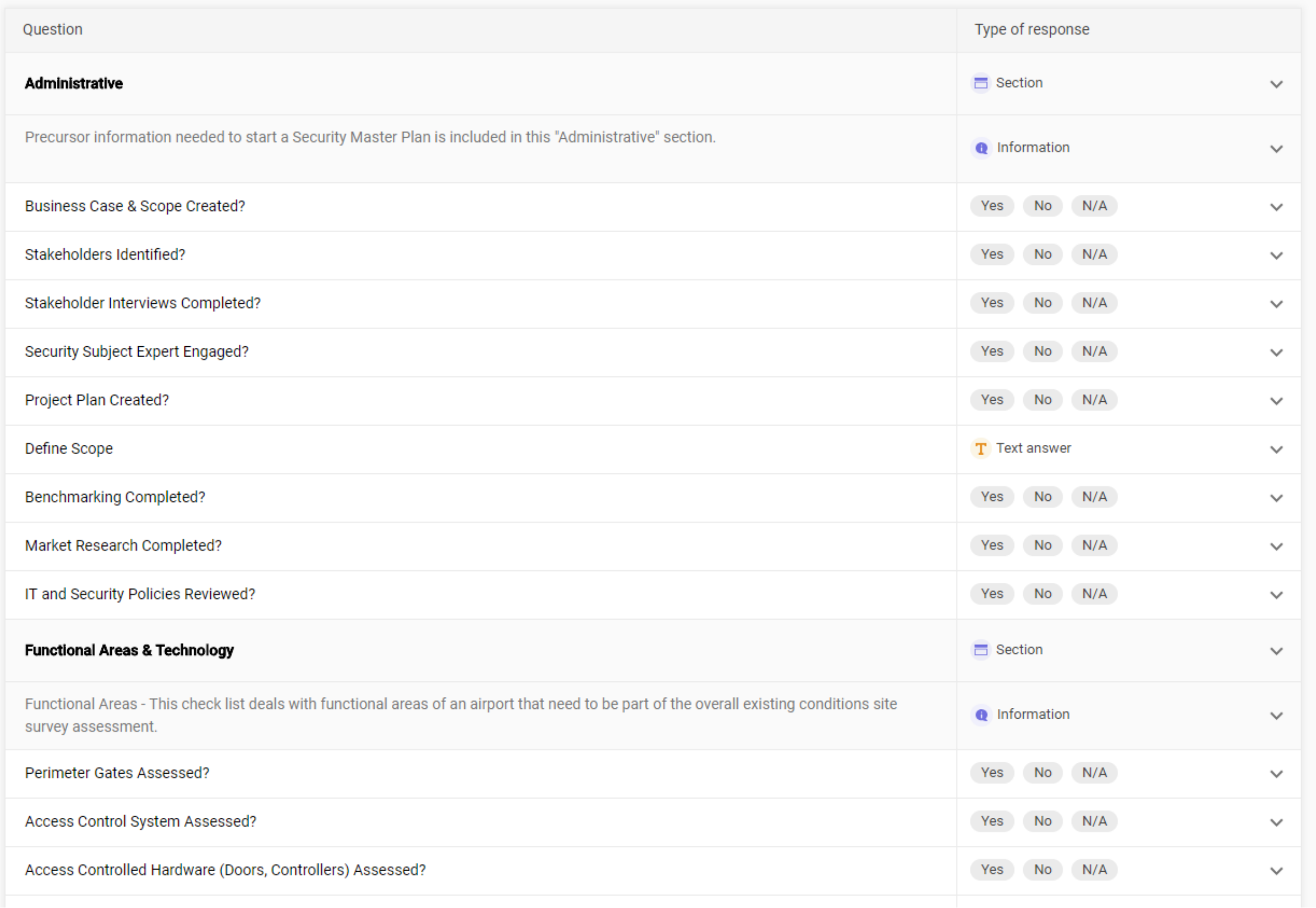
Areas of focus in this section will include:

- Planning tools
- Interviews
- Security department needs assessment
- Site security assessments/site surveys
- Policies, procedures, and directives review
- Asset/inventory baseline
- Milestones and deliverables

5.1.1 Planning Tools

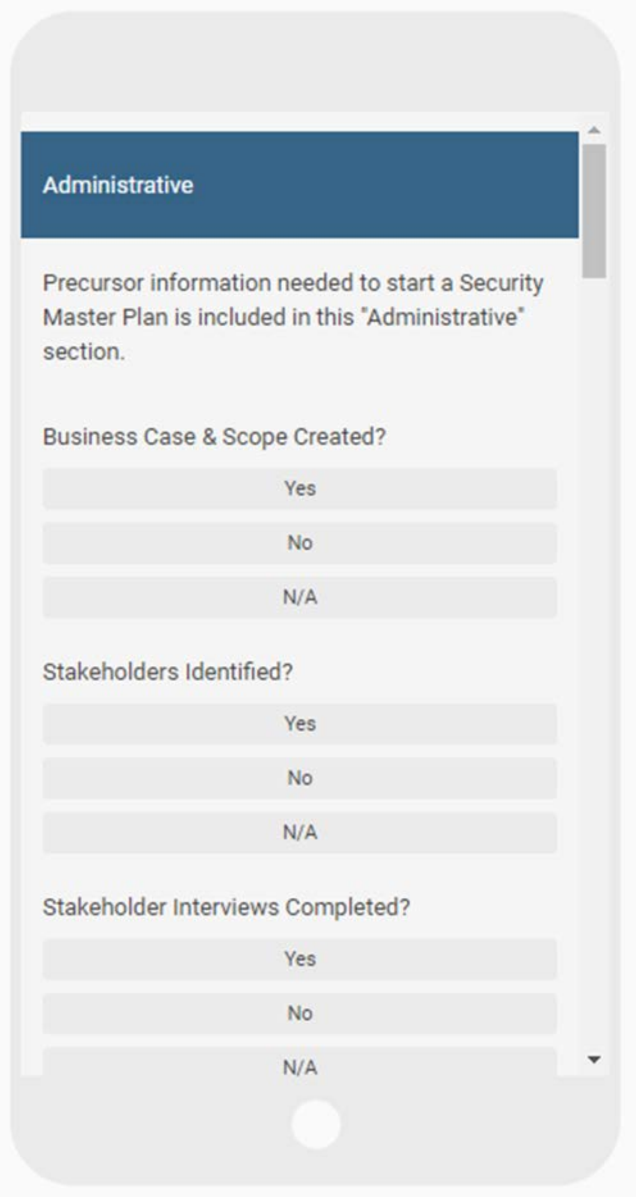
Before starting the SMP process, a good best practice is to have a plan for the use of software applications, computers, devices, and other planning tools to collect data points. Figures 5 and 6 are screenshots from one possible application. These checklists are also available in an Excel spreadsheet found in Appendix J.

Figure 5. Online Planning Tool Used to Create Mobile Device Checklist



Question	Type of response
Administrative	Section
Precursor information needed to start a Security Master Plan is included in this "Administrative" section.	Information
Business Case & Scope Created?	Yes No N/A
Stakeholders Identified?	Yes No N/A
Stakeholder Interviews Completed?	Yes No N/A
Security Subject Expert Engaged?	Yes No N/A
Project Plan Created?	Yes No N/A
Define Scope	T Text answer
Benchmarking Completed?	Yes No N/A
Market Research Completed?	Yes No N/A
IT and Security Policies Reviewed?	Yes No N/A
Functional Areas & Technology	Section
Functional Areas - This check list deals with functional areas of an airport that need to be part of the overall existing conditions site survey assessment.	Information
Perimeter Gates Assessed?	Yes No N/A
Access Control System Assessed?	Yes No N/A
Access Controlled Hardware (Doors, Controllers) Assessed?	Yes No N/A

Figure 6. Mobile Device Checklist Example



Administrative

Precursor information needed to start a Security Master Plan is included in this "Administrative" section.

Business Case & Scope Created?

Yes

No

N/A

Stakeholders Identified?

Yes

No

N/A

Stakeholder Interviews Completed?

Yes

No

N/A

5.2 Current State Conditions

This initial phase of the SMP focuses on gaining detailed knowledge of the airport's physical layout, security systems, supporting technology, perimeter, supporting infrastructure, processes, and policies. This important knowledge is captured and documented to gain buy-in from the process's key stakeholders and serves as the baseline and reference material during the gap analysis and recommendations. Current state conditions can be captured using various methods described below, and project leads can disseminate the information to stakeholders to build a quality, implementable roadmap. An example of an Existing Conditions outline for an SMP can be found in Appendix E.

5.2.1 Interviews

Stakeholder interviews are an excellent method to collect and understand the current state of an airport from the stakeholder's view. Two approaches to interviews are recommended. The first includes various airport stakeholders who work with security aspects but are not necessarily the security department staff or executive management. They know best what is working and what are the security pain points and potential needs. Interviews with various internal and external stakeholders at an airport will be done as part of the SMP current conditions assessment and will include but not be limited to key staff, tenants, and external groups. The second approach is to interview the staff members directly responsible for security and the executive oversight team.

The types of questions asked as part of these interviews will vary depending on the audience, organizational goals and objectives, and the vision of the SMP, but all will have an underlying theme. A sample list of potential stakeholder questions is included in Section 4.3, but this sample should be tailored by the interviewers for each interview session conducted based on the attendees' subject matter expertise.

5.2.2 Security Department Needs Assessment

Once internal/external stakeholder interviews are accomplished, then internal assessments between executive management and the various security department roles should be conducted. Table 1 provides the areas of focus that should be covered when interviewing the executive team, security management, and staff. The questions should be tailored appropriately and may include but not be limited to the following:

Table 1. Example Interview Questions

RESPONDENT INFORMATION	
Title, Role, and Responsibilities:	
Department/Functional Area:	
Years of experience as it relates to airport security:	
Number of Direct Reports:	
Additional skillsets or training needed to keep up with the demand and responsibilities regarding airport security (if any):	
Adequacy of time or resources to perform your airport security-related responsibilities:	
SECURITY STRATEGY	TARGET AUDIENCE
What is the long-range vision for airport security?	Executive Team
Can you measure the performance of airport security operations today in terms of metrics? What metrics do you collect? How frequently? How are they stored/accessed?	Executive Team and Department Heads
Are there additional metrics you believe you need to better manage your security operations?	Executive Team and Department Heads
Do you believe your airport security management reporting system is adequate? If not, why? What is missing?	Executive Team and Department Heads
When you think about security at your airport, where is the biggest need for improvement (e.g., technology, collaboration, procedures, skills, regulations, etc.)?	Executive Team and Department Heads
Based on aviation trends, consolidation of airlines, and growth in international traffic, how do you see the airport operating differently in the next 3–5 years?	Executive Team
What preparations can the airport make now to best prepare to meet the operating challenges of the next 3–5 years?	Executive Team
ORGANIZATION, STAFFING, SKILLS	TARGET AUDIENCE
In terms of the Aviation Security Department organization structure, what works well today? What (if anything) could be improved?	Executive Team and Department Heads
Are current skillsets enough for performing operational responsibilities?	Department Heads
Are there any future reorganization plans that would impact the Security Department?	Department Heads
Are current number of resources enough for current workload demands? How do projected future needs impact resource requirements?	Department Heads
Do you currently have any hiring restrictions or limitations?	Department Heads
Does your airport's training program or curriculum adequately address security-related topics, skills, capabilities, etc.?	Department Heads
What specific staffing recommendations do you have for improving the efficiency and effectiveness of security at your airport (if any)?	Department Heads
SYSTEMS AND TECHNOLOGY:	
Do you believe airport security systems and technology can beneficially impact airport operations and services?	Executive Team and Department Heads

Regarding airport security systems and technology, is what the airport is doing enough? If not, why not?	Executive Team and Department Heads
Are there any systems you utilize regarding airport security matters? If so, which ones? Do you know when they were installed or last updated?	All Staff
How well are your airport's security-related systems maintained?	All Staff
In terms of meeting operational- and/or security-related needs, are these systems enough? If not, why not?	All Staff
Are there any specific features/functions you would like to see automated or improved via systems or technologies?	All Staff
In terms of security systems and technologies, what are your top 3 priorities for the next 3–5 years?	Executive Team
BUSINESS PROCESSES:	
Are there security-related business process or operational issues that adversely impact individual or business unit's day-to-day responsibilities?	All Staff
Are there any major operational challenges in running the airport today that relate to airport security?	Executive Team
Are your airport's existing security-related business processes automated to the extent necessary? Which processes are the biggest pain points for you/group? Are there any suggested recommendations for their improvement?	Executive Team and Department Heads
To what extent is the Security Department involved in the airport's planning, design, and capital project construction processes? Are formal reviews by airport security properly included where applicable?	Executive Team and Department Heads
AIRLINES, TENANTS, PASSENGERS:	
Are there are any specific airline or other stakeholder challenges that relate to airport security?	Executive Team
Are there any specific passenger challenges that relate to airport security?	Executive Team
In terms of services to your customers—passengers or tenants/airlines—what capabilities or services do you want to improve or implement related to airport security?	Executive Team
What security-related capabilities or services would you want airport tenants and/or airlines to improve or implement (if any?)	Executive Team
FINANCIAL:	
What is the annual operating budget (including internal labor costs) for security-related systems?	Department Heads
What budget constraints (if any) do you currently have? Is the existing budget enough to maintain enough Quality of Service levels?	Department Heads
What security-related capital-budget items do you have? Are they in the 5-year Capital Improvement Plan (CIP)?	Department Heads
Do all your security-related service providers have defined service level agreements (SLAs) in place? Are they tied to any financial incentives/penalties?	Department Heads
Is the existing contracting structure for security-related support adequate?	Department Heads

OTHER:	
What are your goals for the SMP when completed?	Executive Team
In terms of airport security, what airport(s) would you like to mirror in terms of operating efficiencies and management? Why?	Executive Team
How would you describe your airport's relationship with the TSA senior management?	Executive Team and Department Heads

5.2.3 Site Security Assessment / Site Surveys

Building an SMP will differ considerably from conducting a site security assessment. Not only will there be a need to identify the positive and negative information of current systems, programs, policies, and procedures, but there will also be a need to define and develop the corrective actions and long-term strategies for planned and documented recommendations.

> Example: Be mindful of pre-existing agreements. A small airport surveyed mentioned a grandfather clause for an airline-owned security system with "access of convenience."

SMP developers who conduct the site assessment will need to have a thorough understanding of all security aspects inside and outside of facilities, fence lines, and access portals (vehicle gates and passenger gates/doors); the flow of operations within secure areas (inside and outside); and the sequence in entering and leaving secure areas. Areas within the airport boundary that may be secured by a tenant via their own ACS and/or monitored by tenant-owned VSS, or through policies and procedures that have been agreed upon by an airport Exclusive Area Agreement or Tenant Security Program, are important to identify and understand as part of the discovery process. All areas of the airport must be accessible by authorized personnel to ensure that compliance with all security protocols are followed. These site assessments and surveys allow for the opportunity to note conditions of physical security, security systems, operational flows, post orders, and/or policies and procedures to identify any potential gaps or pain points in securing remote facilities and the airport campus. Additional guidance to the functional areas (and technology) are covered in Section 6 of this guidebook.

5.2.4 Technology Review

A review of the existing technology used to support airport security operations is important to identify, detail, and document as part of the current conditions. A list of all the technology supporting security functions and operations should be created that includes system name, system function (or use), system owner, system maintainer, vendor/manufacturer, installed date, condition, software (including version number), and a section for notes. Condition, location, and, as appropriate, firmware version should be included for hardware. The information collected at this stage in the process will help to drive recommendations around technology improvements such as compatibility, upgrading, or end-of-life and replacement decisions. A list of technology types used to support airport security and operations includes but is not limited to:

- 800 MHZ Radios
- Access Control
- Biometric Systems
- CCTV / VSS
- Cellular
- Intrusion Detection
- Lock/Key Management
- Mass Notification System
- Network / Wireless
- Paging System

- Command and Control
- Computer Aided Dispatch
- Designated Aviation Channeling Services
- Document Management
- Fingerprinting
- Fire Alarm / Alarm
- Gate Automation
- Identity Management / Badging
- Integration Platforms
- Payment Systems
- Physical Security Information System
- Security Sensors
- Situational Awareness
- Surface Radar
- Vehicle Permit Systems
- Video Management
- Violation Record Keeping
- Visitor / Escort Systems

It is important that the SMPT also investigate the issues around migrating and/or phasing out any current technology that is potentially at or near its end of life to a new system/solution. As part of this technology review, a high-level technology migration strategy needs to be included. While system migration can be relatively easy to accomplish, it still requires a detailed plan for migration and phasing. A best practice associated with project recommendations for changes in technology must include having test locations, test systems, and education for the end users and other airport stakeholders as needed.

5.2.5 Policies, Procedures, and Directives

Current airport documented policies, procedures, and directives will need to be reviewed and analyzed to determine if any gaps exist within the airport security documents. In addition, airport documents should be compared with any new industry best practices and federal policies or procedures to best determine the most appropriate method of addressing these findings in the SMP. It is also suggested that any security language in the tenant leasehold documents or templates be reviewed to determine whether any potential gaps, operational responsibilities, and/or potential modifications may be required as part of future recommendations that are to be documented in the SMP.

As part of the initial data gathering phase, it is recommended that the SMPT obtain copies of the following listed (typical) documents from the security department.

- Airport Master Plan
- Airport Safety and Maintenance Program ([ASMP] if any have been prepared in the past)
- ASP
- IT Master Plan (if any have been prepared in the past)
- Post orders and/or SOPs used by law enforcement officers and those provided by and/or used by contract security personnel
- Private security contracts
- Security construction standards
- Security design standards
- Security policies
- Security procedures (both formally published and those used internally by the security department)
- Security rules and regulations

- Security system change control standards and/or guidance as it relates to changes to the ACS, cameras, VMS, security boundaries, etc.
- Vulnerability Assessments (either conducted in-house or by outside agencies)

It is also important to determine whether the airport or the security department has instituted any formal security controls or processes associated with changes to the facility, and how security personnel obtain information about planned projects and/or proposed changes to the facility. It should also be determined if a standard security guidance document exists for projects when they go out to bid.

5.2.5.1 Understanding the ASP and Security Governance

A key element in the initial data gathering phase for the preparation of an SMP is for the team to understand the Airport's Security Governance structure and to obtain and understand the ASP. Each federally regulated airport must have an ASP in accordance with 49 CFR § 1542. This requirement comes from 49 CFR § 1542.101 of 49 CFR Chapter XII of the TSA regulations for airports with domestic and international air carrier service. The ASP must be approved by the TSA.

While it is understood that each airport is unique and that security measures vary from airport to airport, every regulated airport must have a program under either 1542.103(a) or under 1542.103(b) to meet these regulatory requirements or exceed them with additional measures beyond the minimums outlined within the document. Each ASP is typically structured to reflect regulatory intent and requirements, which are taken from 49 CFR § 1542 as well as current Airport Amendments issued by TSA headquarters and SDs in effect that often require revisions to portions of ASP.

The ASP documents the facilities, methods, and procedures that are designed to provide for the safety and security of persons and property traveling on an aircraft operating in air transportation against acts of criminal violence, aircraft piracy, and the introduction of an unauthorized weapon, explosive, or incendiary onto an aircraft. Therefore, an ASP contains restricted information subject to the provisions of 49 CFR § 1520.1.

Aviation Security Governance is primarily concerned with providing a framework in which the airport security is controlled, operated, managed, and interactive with other airport departments and stakeholders to achieve its objectives relative to airport security-related issues and airport security management. This governance process forms the framework for the security organization to consistently manage the requirements of the applicable federal regulations, and their translation into specific airport rules, regulations, security standards, requirements, and security-related policies.

5.2.6 Current Airport Projects

During the collection of the existing conditions, the SMPT should reach out to those departments and airport personnel responsible for existing projects, including CIP and smaller projects such as maintenance tasks. Many projects at airports are handled by a Project Management Office; however, at smaller airports, individual staff members may manage their own projects.

Airport projects carry dependencies and constraints, as well as scheduled deliverables. The SMPT will need to evaluate these airport projects to see if they are supportive or coincident efforts and provide prerequisite infrastructure or other financial opportunities that may intersect with proposed recommendations. It will be important to identify these project items, along with project date ranges, costs, and use of airport resources (e.g., staff, systems, network, external vendors, and/or consultants).

An example of a Recommendations Summary Table can be found in Appendix E. Appropriately, the SMPT needs to capture the following information about current airport projects:

- Project start and end date – A project is defined as “a temporary endeavor undertaken to create a unique product, service or result. A project is temporary in that it has a defined beginning and end in time, and therefore defined scope and resources.” (https://www.pmi.org/about/learn-about-pmi/what-is-project-management) Therefore, having an idea of current project roadmaps can help the SMPT and the airport security department or organization identify a potential time in the future to carry out the SMP project.
- Project name and brief description – A project is identified formally by the name it is given and used as a reference during the life of the project. Understanding each project at the airport can assist in the identification of potential dependencies and constraints for future proposed SMP project recommendations.
- Project dependencies and constraints – Dependencies in projects are often defined as a state of existence of an entity or an item such that its stability is dictated by another entity or resource. For example, a project to upgrade the VSS is dependent on the airport’s fiber infrastructure having been built out and ready to support the VSS. A project constraint, on the other hand, is a definite and inflexible limitation or restriction on a project. An example could be an expensive ACS installation project involving a new AOA gate and existing fence line. This installation is time sensitive for the airport to maintain federal regulation compliance. However, the failing fence line is not scheduled for replacement until a separate runway project has begun and the schedules do not match.
- Project critical path items and milestones – A project’s critical path is a sequence of activities that represents the longest path through a project and contains “critical” milestones. Typically, these milestones must be identified and accepted by the airport before the next series of tasks takes place, to ensure the project is on the right path to completion. Often, identification of these project items can provide valuable information as to when NOT to start a new project or endeavor.
- Project funding mechanisms – Gaining an understanding of how projects are funded at an airport can provide insight into how (potentially) the SMP effort can be funded. Taking the time to talk to the airport’s finance or capital funding staff and writing down the different options during the SMP planning effort will help future costing and funding processes.

5.3 Benchmarking

While Benchmarking can be applied against any product, process, function or approach, it is helpful to define the common focal points for benchmarking security at the airport, such as operations, technology implementation, processes, and/or procedures.

The intent of benchmarking is to compare an airport’s security planning with other similar airports to identify best practices and lessons learned; generate ideas for improving processes, procedures, approaches; and use technologies to establish performance goals. Benchmarking is an important component of continuous improvement and quality initiatives, such as Six Sigma.

The SMP will benefit greatly from the results found in the Business Case process of benchmarking. The results will help the airport identify and eliminate gaps or areas that require strengthening (e.g., operations, technology, administrative, etc.)

Benchmarking, as part of the SMP Business Case process, is a powerful tool to aid in the promotion of a need or desired improvement within holistic security planning. It is important that the SMPT work with key stakeholders to define benchmarking initiatives deliberately, or the results can be misleading. While benchmarking methodologies vary, a typical process involves:

1. Defining the security related topics or functions for the benchmarking study
2. Defining the process or attribute to be studied in detail
3. Selecting and defining the measures
4. Selecting the comparison set of at least five similar airports
5. Collecting data on both the benchmarking subject and comparison set
6. Assessing the data and identifying gaps

5.4 Market Research

Categorized as a best practice, "…market research is the process of analyzing data to help understand which products and services will achieve the desired protective system, and how to get the best economic value for the required protective system equipment" (Best Practices for Planning and Managing Physical Security Resources, 2015). Market research can also assist in determining latest system features and benefits, technological advances, and ROM costs.

There are many approaches to conducting market research, including surveys, meetings, phone discussions, webinars with vendors, and web research. As an example, when creating a market research plan or tool, areas of consideration include:

- Estimated hardware and software costs
- Estimated implementation costs of hardware/software
- Overall lifecycle cost of the requested equipment (maintenance and support)
- Estimated cost of employee training and increase in employee productivity
- Compliance with applicable federal, state, and local standards, statutes, and/or policies

The results of market research can be used in planning for updates to Functional Areas and Technology (Section 6) and ROM cost estimates (Section 7) in support of proposed project budgets, while benchmarking data can be used as part of the gap analysis efforts (Section 7). Both tools can support assessing risk (Section 7), along with the information presented from conducting existing-conditions site security assessments (Section 5) and review of existing processes to create a solid SMP foundation.

SECTION 6: FUNCTIONAL AREAS AND TECHNOLOGY

6.1 Introduction

The airport campus is generally referenced as inclusive of landside and airside; however, when discussing security-related areas and the corresponding technology/systems and infrastructure, a more detailed and comprehensive view should be considered. This section will describe the physical areas and technologies that the SMPT members should familiarize themselves with as they prepare to create the SMP. It will explore best practices as to how to document these items using an existing condition, gap analysis, and recommendation framework. Examples of airport documentation framework processes can be found in Appendix E.

PARAS 0010 *Guidance for Protecting Access to Vital Systems Impacting Airport Security* was published in October 2017 by National Safe Skies Alliance. This is an important resource and can provide the SMPT with a larger list of functional areas relevant to the creation of an airport SMP.

An overview of the topical area groupings, areas of evaluation, and associated subsections related to IT items will be included (see below).

6.2 SMP Assessment Organizational Focus Areas

There are multiple ways for the SMPT to review and analyze the airport and its security organization, systems, programs, plans, and processes to present the resultant analysis and recommendations. This can be accomplished by grouping the analyzed data by either Functional Area or Physical Area. Best Practice dictates that each topical area be thoroughly reviewed, with appropriate recommendations made in support of both aspects, regardless of how the SMPT determines they wish to organize and present the results. See Appendix I for an example of a recommended roadmap grouping recommendations by Physical or Functional areas.

6.2.1 Functional Areas

This section lists the typical security-related Functional Areas to be included in evaluation and risk assessment (Section 8) when doing site security survey work and observations. Interviews, site surveys, and observations should be well documented, including photographs, for future gap analysis and recommendations.

- Security organization and administration documents
- Staffing and resources available
- Airport security operations policies and procedures
- Regulatory documents
- Security system and technology inventories
- Infrastructure inventories
- Airport policy/procedural documents

6.2.2 Physical Areas

This section guides the SMPT to the most common Physical Areas to be included in evaluation and risk assessment (Section 8) when doing site security survey work and observations. These surveys should be well documented, including photographs, for future gap analysis and recommendations.

- Terminal complex including public areas
    - Arrival and departure curbside sidewalk areas
    - Ticket lobby and counter areas
    - Parking structures abutting the airport’s arrival and departure roadway and curbside areas, including roadways associated with close-in parking
    - Protective bollards at facility entrances including arrival and departure curbside sidewalk areas
    - Ground transportation drop-off/pick-up
    - Vehicle inspection areas
    - Employee transportation systems
    - Taxi and app-based ride share hold-area parking lots
    - Cell phone waiting lots
- Storm drains and outfall structures
- Critical infrastructure
    - Communication centers
    - Central utility facilities
    - Underground tunnels and pathways connecting spaces
    - Power distribution and backup power sources
- Security operations
- Airport/airfield operations
- IT facilities, server rooms, and critical telecom rooms
- Law enforcement and ARFF facilities
- Facilities/maintenance
- Physical security barriers
- AOA boundary and gates
- Cargo operations
- Fixed Base Operator and/or general aviation (GA)

6.3 Technology and Infrastructure

Technology systems, networks, and infrastructure are a critical piece of any airport security system and should be considered a key functional area. Traditional areas of technology include computer workstations, servers, software, networks, and network devices such as switches, cable infrastructure, data centers, and telecommunication rooms.

Often, the SMPT will find the airport security department or organization is the owner of the security system and thus sets requirements and standards for it. These security systems typically utilize the airport’s IT department or organization’s cable and/or network infrastructure for interconnection and communication. At many airports, computer servers are likely supporting these dedicated security systems in airport IT data centers. At some airports, support for security systems such as the ACS and/or the VMS is managed and controlled solely by the security department; at others, it is managed by the IT department. There may be an informal, undocumented arrangement that covers some level of shared responsibility.

Sometimes the division of roles and responsibilities associated with security systems, technology, and related infrastructure is not clear and may not be well documented. Best practice dictates that the SMPT obtain detailed documentation on roles and responsibilities and interview both the security and technology departments or organizations for security systems, technology, network infrastructure, systems ownership, change authorization, change management, systems support, and lifecycle replacement.

This section briefly describes each typical area and gives recommendations on how to proceed with the overall design considerations and planning of change management and lifecycle replacement.

6.3.1 Computers and Workstations

Computer servers and workstations serve as the heart of any security system, as they provide the primary interface to the end user for security-related content. Identification of these assets is key and relevant to the creation of an SMP.

- Existing conditions research – Will confirm information on the number of current workstations and servers needed in accordance with the number of users. Document current state and compare with future goals.
- Monitors and video walls – Must be considered for the best application of viewing real time content and assisting with situational awareness. Document whether the current state matches future goals.
- Technology outages – Workstations and servers need care and maintenance. Vulnerabilities in software applications and operating systems require patching. For example, a common term in the IT industry, Patch Tuesday, stems from Microsoft application patches coming out every Tuesday. Document the airport’s current preparedness for these patches.
- Physical security of the work areas – These work areas are critical and need to be secured. Consider the use of cameras monitoring the entrance and exits as well as an access control system.

6.3.2 Network and Logical Security

Network and logical security technology are a key consideration for SMP development. Modern IP networks are now considered critical infrastructure required for airport operations, security, maintenance, and multi-domain collaboration. Typical designs provide not just a communication backbone, but enterprise services, enforcement of security policies (physical and logical), distributed processing, distributed storage, real-time analytics, and reporting, which are all directly affected by requirements and constraints of physical security system components.

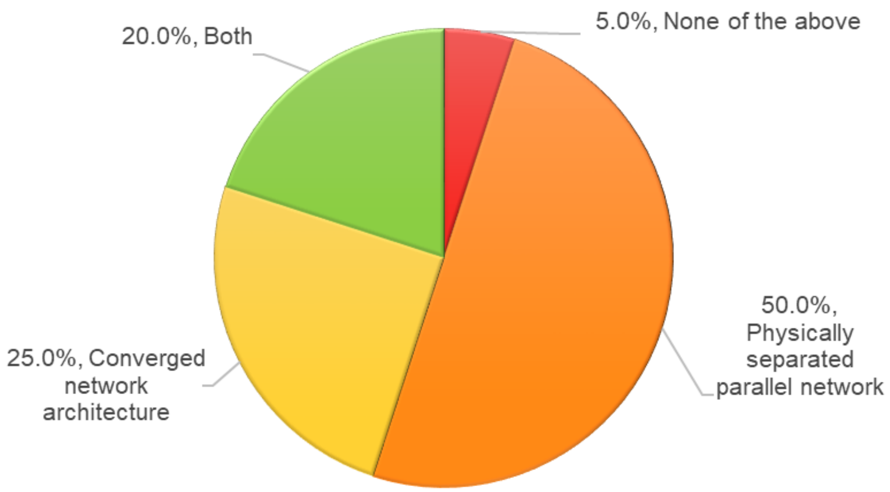
The planning and design of physical security systems must first evaluate existing conditions for network and logical security design and policies. Once this is accomplished, a gap analysis can be conducted comparing the current state of design requirements and constraints to future goals.

6.3.3 Network Architecture

Physical security system requirements and constraints are key network architecture considerations and commonly drive the need for network improvement and refresh projects. Physical security systems have become critical to not only security departments but for operations groups as well, and rely on enterprise IT system integration like any other tenant. A Best Practice is to determine to what level the airport’s physical security systems (ACS, PIDS, and VMS) are documented in the ASP. This would include any security department commitment within the ASP to maintain physically separated networks.

In 2018, 19 airports were surveyed on their specific network architecture type. As shown in Figure 7, 50% responded that their security network was physically separated and parallel to their regular business network (e.g., business applications, e-mail, and web browsing). Of the 19 respondents, 25% indicated the two networks were “converged” logically, while 20% stated they have both converged and physically separated networks.

Figure 7. Network Architecture Type



Understanding network architecture can affect accessibility to certain systems in security, the areas of focus listed in Table 2 are advisable to consider:

Table 2. Network Architecture Areas of Focus

Area of Focus	Examples
Physical Security system integration requirements with IT Enterprise systems	Active Directory and Geospatial Information Systems
Remote access requirements	Including vendor support/maintenance and airport’s internal staff
Network performance requirements	Including bandwidth, latency, availability
Network redundancy requirements	Cloud, Local Storage, or Combination
Network impact evaluation	Including impact to other critical systems
Software multitenancy considerations	
Network protocol requirements	e.g., Transmission Control Protocol/User Datagram Protocol, Multicast, Smart Network Management Protocol, Network Time Protocol, etc.
Consideration for ongoing and planning CIP	

6.3.4 Network and Information (Cyber) Security

Information Security is defined as “the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability” (National Institute of Standards and Technology, (NIST) *An Introduction to Information Security*, June 2017). Networked physical security systems and their associated communications need to be logically secured, monitored, and able to respond to threats to ensure confidentiality, integrity, and availability of critical systems and data.

> For a more in-depth look at protecting network security systems and the physical locations where they reside, consider reviewing National Safe Skies Alliance PARAS 0010 *Guidance for Protecting Access to Vital Systems Impacting Airport Security*

An SMP must include both physical and logical security projects and technology, especially considering many network refreshes have moved the aviation industry towards a converged network architecture, with physical security, administration, and sometimes building management networks riding on a shared infrastructure. This decision is typically driven by the need to reduce management overhead, maintenance costs, and accommodate the latest tenant system requirements. Having multiple tenants on a network exacerbates the need for protection and insight of airport networks, with the following areas of focus as examples for consideration:

- Traffic segmentation
- Network access control
- Zero-trust policies
- Security information and event management
- Intrusion detection and prevention
- IT system authentication methods
- Policy enforcement and auditability

6.3.5 Monitoring and Maintenance

Active monitoring and proactive maintenance of systems is important to the overall health of a successful security system, and include the following best practices:

- Change management
- Patch management
- Planned outages
- Emergency outages
- Disaster recovery
- Business continuity

6.3.6 Best Practices for Software Procurement and Implementation

Procurement of security software, hardware, and associated networking is made up of a series of activities and procedures that are often combined into a single process. One example—Best Value Procurement, which is high-level approach to procurement—will include a sophisticated understanding and application of methods to achieve best value while balancing multiple factors regarding costs, quality, and risk. Methods in Best Value Procurement may include Total Cost of Ownership analyses, and performance-based contracting or design-build (e.g., construction contracting and project delivery). These methods tend to maximize efficiency in the procurement process and, at the same time, enhance creation of procurement documents, such as the RFP, which includes requirements that have been vetted by the system owner, users, and stakeholders.

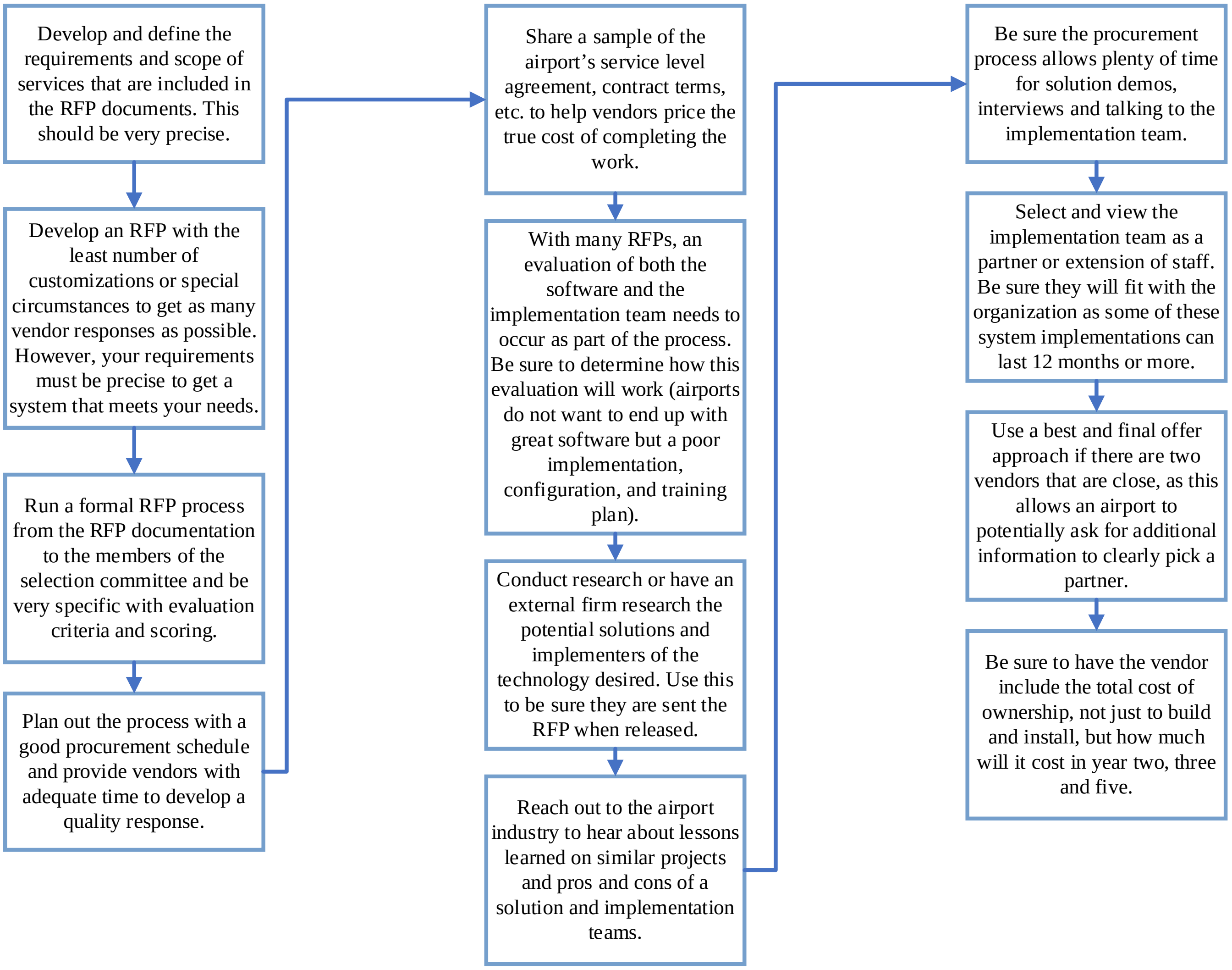
Procurement at an airport can often be a lengthy process. Airports must comply with internal, local, and/or federal government rules and regulations around how goods and services are purchased. Often, changes to security systems will require modification updates (amendments) to the ASP. These amendments require TSA approval.

While the typical SMPT will not be expected to prepare an RFP, the team will most likely contribute to the information contained therein, and should have a clear understanding of the procurement process to properly document not only the need for a new and/or replacement system, but also the potential costs and timeframe associated with procurement at the airport. To obtain this background information, the SMPT will need to include additional interviews with the airport’s procurement and/or acquisitions team, often including members of the airports planning and development group. In keeping with SSI control requirements, the SMPT will need to work with the airport’s procurement specialist and the ASC to ensure proper controls exist during the bid process. At airports where request for qualifications (RFQ) processes are authorized, an RFQ should be issued in advance of the RFP so that vendors from the RFQ process can be invited to propose after signing an SSI Non-disclosure Agreement. Prequalifying vendors will be based on detailed requirements designed by the airport.

Developing a detailed RFP can be done internally or with the help of professional services.

Figure 8, the RFP Development Flow Chart, guides an airport through a best practice of developing and advertising an RFP. There are several steps and recommendations for developing the RFP document, as well as selection criteria and costing considerations. Understanding the RFP process, along with the associated ROM costs and implementation timeframes related to a new and/or replacement security system or service, is critical when developing the project recommendations.

Figure 8. RFP Development Flow Chart



Develop and define the requirements and scope of services that are included in the RFP documents. This should be very precise.

Develop an RFP with the least number of customizations or special circumstances to get as many vendor responses as possible. However, your requirements must be precise to get a system that meets your needs.

Run a formal RFP process from the RFP documentation to the members of the selection committee and be very specific with evaluation criteria and scoring.

Plan out the process with a good procurement schedule and provide vendors with adequate time to develop a quality response.

Share a sample of the airport's service level agreement, contract terms, etc. to help vendors price the true cost of completing the work.

With many RFPs, an evaluation of both the software and the implementation team needs to occur as part of the process. Be sure to determine how this evaluation will work (airports do not want to end up with great software but a poor implementation, configuration, and training plan).

Conduct research or have an external firm research the potential solutions and implementers of the technology desired. Use this to be sure they are sent the RFP when released.

Reach out to the airport industry to hear about lessons learned on similar projects and pros and cons of a solution and implementation teams.

Be sure the procurement process allows plenty of time for solution demos, interviews and talking to the implementation team.

Select and view the implementation team as a partner or extension of staff. Be sure they will fit with the organization as some of these system implementations can last 12 months or more.

Use a best and final offer approach if there are two vendors that are close, as this allows an airport to potentially ask for additional information to clearly pick a partner.

Be sure to have the vendor include the total cost of ownership, not just to build and install, but how much will it cost in year two, three and five.

SECTION 7: DEVELOPMENT AND ACTION PHASE

7.1 Introduction

In this section, industry-proven tools and techniques are applied to analyze the gaps and weaknesses that may exist in an airport's current security programs, systems, and processes to determine what vulnerabilities they may pose, and the discrete action plans required to address them. The resultant SMP recommendations guidance will help security management assess: 1) the potential threats to their airport; 2) the airport's vulnerability to the identified threats; and 3) the consequences that can result from a successful exploitation of those vulnerabilities.

Several commercial airports have already begun to proactively assess their security vulnerabilities and in doing so have provided general best practices in technology, organizational, physical and process-based approaches to addressing them. These best practices can provide guidance on many of the crucial steps involved in developing an SMP, including approaches to assessing risk and vulnerability to airport operators through surveys, meetings, phone discussions, and web research. As a guideline, functional areas and groups identified in Section 6 will be used as a baseline for managing gaps and risks.

7.2 Design Constraints, Desired Functionalities, and Functional Requirements

Prior to going through the gap analysis effort (but an essential component of it), information received as feedback from stakeholder interviews, surveys, and the existing conditions data collection needs to be processed and analyzed. In this subsection, the captured and categorized feedback will be used to determine and/or establish Desired Functionalities and Functional Requirements.

- "Design Constraints refers to 'a limitation on a design.' It includes imposed limitations that one does not control and limitations that are self-imposed as a way to improve a design" (Simplicable, 2017).
- Desired Functionalities are those requests, recommendations, and needs compiled through stakeholder interviews and surveys.
- Functional Requirements include rules imposed by the airport's local policies and/or local, state, and federal laws and regulations.

The above three data sets be categorized for easier evaluation through use of the following four criteria:

- Regulatory – Documentation of current regulations must be gathered and incorporated. This includes FAA, CBP, and TSA, as well as airport-specific regulations. In cases where regulations differ per regulatory authority, the stricter of the corresponding regulations should be followed.
- Operational – Operational impact of proposed or contemplated solutions.
- Passenger Experience – Potential impacts of increased security practices on passenger experience.
- Functional – Functional Requirements should be determined. This would include system functionality, which could potentially address or mitigate impact on operational or passenger experience information gathered previously, e.g., integrations, leveraging of existing systems, and combining of existing systems.

The results of this effort feed directly into the activities described in the gap analysis and risk assessment section.

7.3 Gap Analysis and Risk Assessment

A gap analysis compares two things to measure the difference between them. Often a gap analysis helps in comparing two different states of something—the current state and the future state. Once the gap is identified, one can look for ways of bridging the gap.

For an SMP, a gap analysis is a method that the SMPT can use to measure the difference between the current state of the airport security department's policies, processes, procedures, staffing, security systems and infrastructure and their anticipated future (desired) state. For those who might see a negative connotation in the term gap analysis, this method can be also be termed opportunity analysis, needs analysis, or needs assessment.

Performing this analysis involves comparing **what is**, with **what should be**. What should be can be determined from:

- Comments expressed to the SMPT from the security department staff and leadership during interviews
- Benchmarked and/or similar airports
- Industry standards
- Aviation security best practices

A gap analysis takes into consideration the Design Constraints, Functional Requirements, and Desired Functionalities developed in the prior section, and formalizes the results into manageable gaps to analyze and begin vulnerability planning efforts. An example framework for a gap analysis report would include the following components:

Identified Gap: Perimeter Surveillance

- Functional Area – Terminal and airport campus
- Technology Area – Network infrastructure, data center, server, software, and licenses
- Existing Condition – VSS cannot observe the perimeter
- Design Constraints
    - The VSS cameras are older and not placed in range of the perimeter
    - The network infrastructure does not reach portions of the perimeter
- Functional Requirements
    - Airport policy requires response times of less than XX minutes to an incident on the airport campus
    - Airport's strategic initiative defines world class safety and security as a major initiative
- Desired Functionalities
    - VSS at all vehicle and pedestrian gates on the perimeter
    - Real-time situational awareness using proven technology such as Unmanned Aircraft System and/or fence intrusion detection

An example gap analysis report summary is shown in Table 3.

Table 3. Example Gap Analysis Report Summary Table

Item #	Identified Gap	Relative Priority	Business Process	Organization	Technology	Physical
1.0	**Airport Security Related**					
1.1	Perimeter Surveillance	**Medium**	Consider AMP and the need to optimize perimeter security. Establish standards for perimeter surveillance.	Ownership of a safe/secure airport campus perimeter and surveillance capabilities governed by a committee of airport individuals in security, operations, and IT.	Technology infrastructure, software, and hardware, including upgrades to cameras, are part of the overall assessment.	Currently limited power and communications infrastructure, mostly around existing buildings and gates. This would need to be supplemented.

As a subsequent exercise, a risk analysis, risk assessment, and risk mitigation planning effort of the SMP builds upon the identified gaps. Sections 7.3.1 and 7.3.2 provide an overview of a vulnerability review and the application of a threat and vulnerability assessment and mitigation plan. As an introduction, it is important to distinguish between the definitions of threat, vulnerability, and risk to understand how they are applicable to this process:

- A threat can be in a physical and/or technical (computer/network) context and refers to anything that has the potential to cause harm or damage.
- A vulnerability can be in a physical and/or logical (computer/network/process/procedure) context and refers to a weakness that allows a threat actor/agent to exploit a secured area (e.g., airport perimeter, computer application, system database, or physical telecommunications infrastructure).
- Risk = Threat (times) Vulnerability. Risk refers to the potential for loss or damage when a threat exploits a vulnerability. Examples of risk include financial loss because of business/security disruption, loss of privacy, reputational damage, legal implications, and even loss of life.[1]

7.3.1 Vulnerability Review Exercise

Airports can begin a vulnerability review exercise by performing a self-administered risk assessment using a TSA-provided template. This activity will survey existing conditions and identify vulnerabilities throughout the airport. Using the Project Management Plan as a baseline document, existing knowledge of facilities, stakeholders, and internal processes will benefit operators as they scan for vulnerabilities in areas such as the airport's own IT network and communications systems, baggage systems, ACSs, parking management systems, VSS/CCTV, PIDS, eEnabled aircraft systems, document management systems, and radar systems. The SMPT should request copies of any vulnerability review exercises

[1] Adapted from: bmc blogs, https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/, *IT Security Vulnerability vs Threat vs Risk: What's the Difference?*, Stephen Watts, June 21, 2017

undertaken by the airport, or any vulnerability assessments performed by outside groups or agencies at the request of the airport to compare the process and outcomes to this review exercise.

7.3.2 Threat and Vulnerability Assessment and Mitigation Planning

An SMP cannot make recommendations for future planning of security programs that will be effective unless the resultant programs are based upon an understanding of the risks it is designed to control. Threat, vulnerability, and risk are all factors related to airport security. It is important that the SMPT and the airport have a common understanding of the definition of these terms. An airport Threat and Vulnerability Assessment (TVA) is a key tool in determining the extent to which an airport facility may require security enhancements to systems, infrastructure, processes, and/or procedures.

The terms threat and vulnerability cover a wide array of events, some of which cannot be eliminated while still operating the system. Since no system can be rendered totally secure, the impact of identified threats and vulnerabilities must be assessed to determine whether the risk of their occurrence is acceptable, and the extent to which corrective measures can eliminate or reduce their severity and/or likelihood of happening.

Threats can be defined as specific activities that can damage the airport and its facilities, and cause employee and/or passenger injury or death. Threats include any actions that detract from the overall safety and security of the airport and its operation. A threat can include a bad actor (an insider or outsider) who may wish to cause harm, ranging from extreme examples of terrorist-initiated bombs or hostage-taking to common events such as theft of services, gun and drug trafficking, pick-pocketing, graffiti, and vandalism.

A **vulnerability** can be defined as a weakness or gap in an airport security system, program, and/or process that can be exploited by threats to gain unauthorized access to an airport asset or leave the airport susceptible to some form of security hazard.

Risk (the potential for loss, damage, or destruction of an airport asset) occurs when systems, processes, and procedures have a **vulnerability** that a given **threat** can exploit or attack.

When the SMPT or an internal airport security team conducts a TVA, those responsible for identifying and assessing threats and vulnerabilities must not only measure the degree of potential harm, but the chances of that harm occurring. This assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in an airport security system, process, and/or procedure.

Risk therefore is the intersection of **assets**, **threats**, and **vulnerabilities**. The formula used to determine risk is; A + T + V = R. That is, Asset + Threat + Vulnerability = Risk. **Risk** is a function of **threats** exploiting airport **vulnerabilities** to obtain, damage or destroy **airport assets**.

The primary objective of an airport TVA is to observe and analyze areas of potential and/or actual vulnerability, to define causes, and to recommend means to reduce or eliminate exposure. The assessment should include a review of all airport facilities, security boundaries, critical infrastructure, security systems, programs, processes, and procedures.

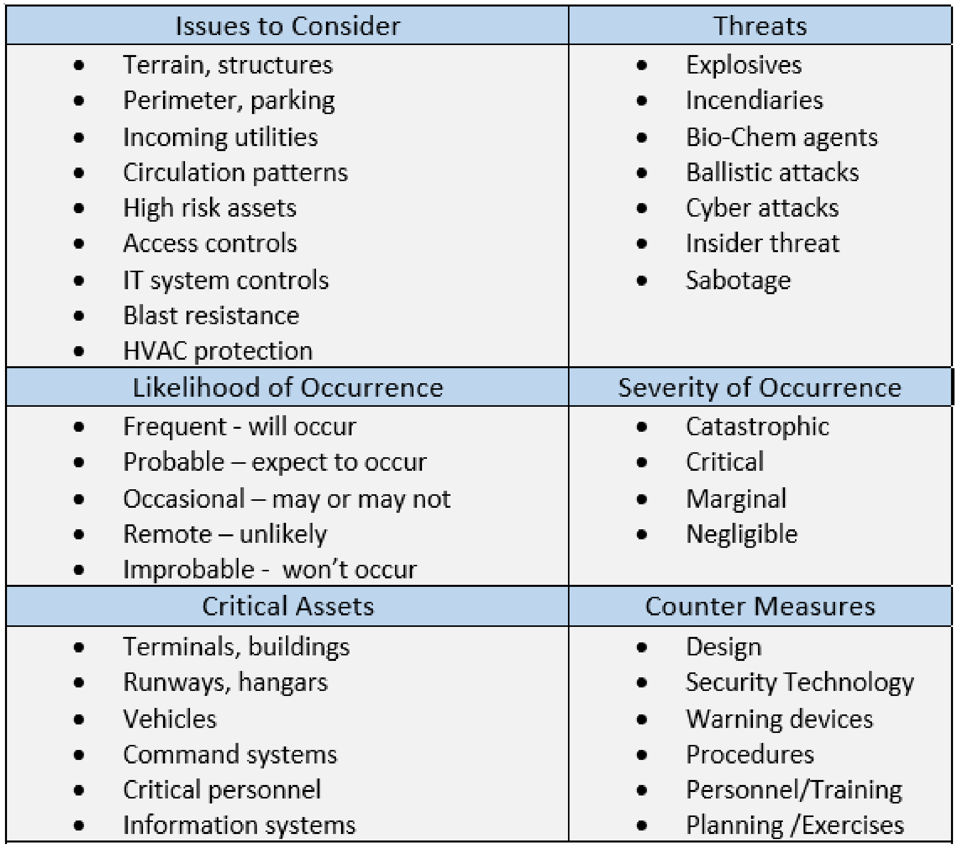
There are many tools, guides, and methodologies available for conducting a TVA. See Figure 9, which depicts a Model for Assessing Vulnerabilities as a starting point and guide.

This document also offers some examples in Appendix F: Airport Risk and Vulnerability Assessment Resources. However, all are subjective to varying degrees. The SMPT (or the airport, if an internal assessment is to be made) must be able to answer the following questions:

- “What is the threat?”
- “What is an airport’s level of vulnerability relative to that threat?”
- “To what extent will the threat/vulnerability change?”

Utilizing scenarios specific to an airport are at the heart of assessing vulnerabilities. Table 4 shows how understanding existing conditions, critical assets, and threats feeds into relatable scenarios. The output of the scenarios leads to the scoring mechanisms of probabilities and considerations that guide the user to a likelihood and severity scoring matrix. Understanding the threat allows an airport to apply a practical mitigation plan. It is nearly impossible to remove a threat entirely.

Table 4. Model for Assessing Vulnerabilities

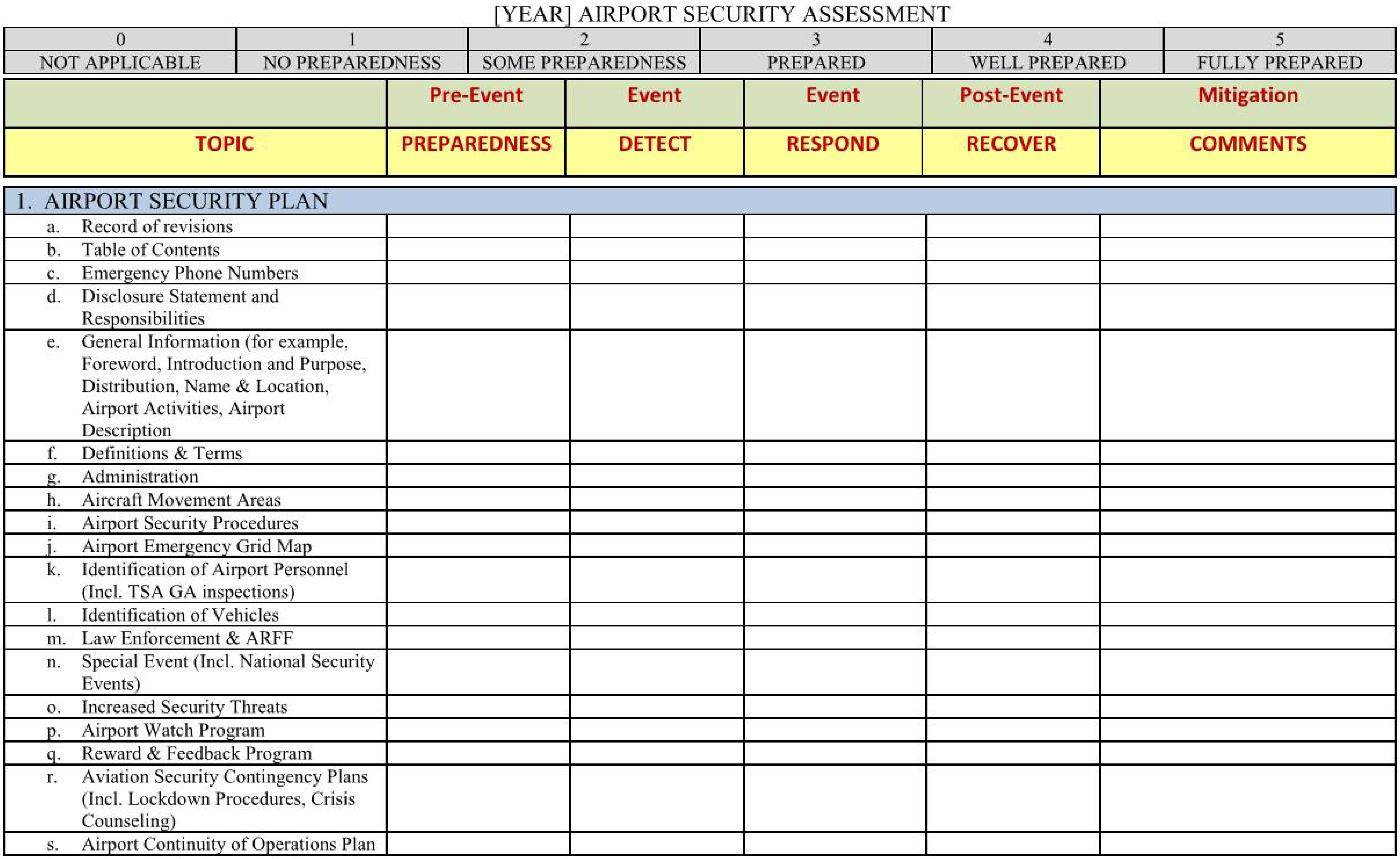


Issues to Consider	Threats
• Terrain, structures • Perimeter, parking • Incoming utilities • Circulation patterns • High risk assets • Access controls • IT system controls • Blast resistance • HVAC protection	• Explosives • Incendiaries • Bio-Chem agents • Ballistic attacks • Cyber attacks • Insider threat • Sabotage
Likelihood of Occurrence	**Severity of Occurrence**
• Frequent - will occur • Probable – expect to occur • Occasional – may or may not • Remote – unlikely • Improbable - won’t occur	• Catastrophic • Critical • Marginal • Negligible
Critical Assets	**Counter Measures**
• Terminals, buildings • Runways, hangars • Vehicles • Command systems • Critical personnel • Information systems	• Design • Security Technology • Warning devices • Procedures • Personnel/Training • Planning /Exercises

Source: National Safe Skies Alliance – PARAS 0004

Another tool is the Airport Security Assessment and Protective Measures Matrix, which is an assessment instrument typically used by GA airports that can help develop a baseline on the status of existing security measures and the priorities for airports. The matrix allows operators to subjectively score their airport in the focus areas listed below across three stages: (a) pre-event preparedness, (b) detection and response during an event, and (c) post-event recovery (Security Guidelines for GA Airport Operators and Users, 2017). Table 5 is an example of the matrix, including the specific focus areas that comprise the assessment. This matrix may be helpful for small airports with limited commercial air service or those that are just beginning the process for the SMP. A complete version of the matrix is provided in Appendix F.

Table 5. Airport Security Assessment and Protective Measures Matrix (sample – see Appendix F)



[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	PREPAREDNESS	DETECT	RESPOND	RECOVER	COMMENTS
1. AIRPORT SECURITY PLAN					
a. Record of revisions					
b. Table of Contents					
c. Emergency Phone Numbers					
d. Disclosure Statement and Responsibilities					
e. General Information (for example, Foreword, Introduction and Purpose, Distribution, Name & Location, Airport Activities, Airport Description					
f. Definitions & Terms					
g. Administration					
h. Aircraft Movement Areas					
i. Airport Security Procedures					
j. Airport Emergency Grid Map					
k. Identification of Airport Personnel (Incl. TSA GA inspections)					
l. Identification of Vehicles					
m. Law Enforcement & ARFF					
n. Special Event (Incl. National Security Events)					
o. Increased Security Threats					
p. Airport Watch Program					
q. Reward & Feedback Program					
r. Aviation Security Contingency Plans (Incl. Lockdown Procedures, Crisis Counseling)					
s. Airport Continuity of Operations Plan					

Source: TSA, Information Publication A-001, Version 2, July 2017, Security Guidelines for General Aviation Airport Operators and Users

This checklist template is intended to help airport operators prepare their internal threat assessment with a consistent evaluation of designs at various levels. The checklist can be used as a screening tool for the design of early stage vulnerability plans. Program and/or design improvement recommendations are to be formulated for any category that the airport deems as underprepared. A project example illustrating results of the threat assessment is provided below:

Project Example and Assessment Process

- Study: Test of physical perimeter security
- Basis of Design:
    - Measure reaction times to perimeter fence breach
    - Measure delay in response times
    - Measure weakness and ability to penetrate physical barrier (i.e., fence)
    - Conduct Blast Mitigation study (reference National Safe Skies Alliance PARAS 0014 *Blast Mitigation Strategies for Non-Secure Areas at Airports* report)
- Design and Contract Administration
    - Design-basis threat report
    - Physical protection assessment techniques
        - Quantify random vehicle inspections
- Program Improvement
    - Threat reduction measures
    - Threat awareness education
    - Appropriate security boundary design
- Financial and Other Considerations
    - Cost of installing new barrier equipment, maintenance of equipment, and education and training of staff on new boundary measures and right of way
    - Overall lifecycle cost of the requested equipment (maintenance and support)
    - Estimated cost of employee training and increase in employee productivity
    - Compliance with applicable federal, state, and local standards, statutes, and/or policies

7.3.3 Additional Resources

To successfully assess risk and vulnerability, several tools can be used, including those in commercially available products. Airports undertaking this effort must understand that an unstructured and fragmented assessment may only make framing the threats, risks, and vulnerabilities more difficult. When using a risk and vulnerability tool, a best practice would be to utilize the existing conditions assessment and the identified gaps as a starting point.

Table 6 contains examples of risk assessment frameworks, methodologies, and tools that various airport stakeholders can use.

Table 6. Internal Vulnerability Plans and Procedures

RISK ASSESSMENT FRAMEWORKS	RISK ASSESSMENT METHODOLOGIES	RISK ASSESSMENT TOOLS
NIST Guide for conducting Risk Assessments	Pugh Methodology	Self-Vulnerability Assessment Tool (SSI) - 2010
	Facilitated Risk Analysis and Assessment Process	TSA Outcome Focus Compliance - 2017
NIST Performance Measurement Guide for Information Security	Central Computing and Telecommunications Agency	Commercial Airport Resource Allocation Tool (SSI) - 2010
TSA Joint Vulnerability Assessments and Protective Measures Matrix	Operational Critical Threat, Asset and Vulnerability Evaluation	Airport Security Self-Evaluation Tool Users' Guide (SSI) - 2011
ASIS International, Security Risk Management Assessment	Risk Analysis and Management Method Methodology	Compliance Security Enhancement Through Testing
National Critical Infrastructure Protection Plan Risk Assessment Framework	Dempster-Shafer Theory of Belief Functions for risk analysis of information systems security	Technology-based Assessment Tool for PIDS

7.4 Project Recommendations, Roadmap, Prioritization, Cost Estimating, and Spend Plans

In this section, the actual SMP takes shape in the form of recommendations. The SMP is intended to create a high-level plan of projects, priorities, and project budgets. These recommendations close any gaps, vulnerabilities, and weaknesses discovered during the process detailed in the earlier sections. The key to building a successful SMP for the security department and airport management is for these recommendations to be ranked relative to the airport's needs to set priorities. ROM cost estimates are established for each recommendation. This information is then used to establish a recommended project road map, which should be overlaid with a yearly projected-spending plan.

The process for developing and establishing recommendations comes from the results of the existing conditions surveys, observations, interviews, gap analysis, and the TVA. The SMPT should develop recommendations from a combination of security measures that may include physical methods, systems, processes and/or procedures. Recommendations should be configured in a methodical framework to best document the affected systems and/or processes. See Appendix F for examples of these frameworks, which include the elements that form the SMP recommendations and project summaries, estimated ROM costs, and estimated time to accomplish the recommended effort. A best practice when establishing a roadmap is to include a spend plan to best convey to airport management the overall costs and costs budgeted by year.

Types of projects may include:

- Study/assessment
- Basis of Design/Project Charter
- Design and Contract Administration
- Physical and architectural additions and/or modifications
- Technology enhancements and/or replacements

- Programmatic
- Organizational changes

It is recommended that, whenever possible, the SMP should be developed in parallel with an Airport Master Plan Update. Ideally, the Airport Master Plan Update would have a section that reviews and discusses technology and security systems; however, while Airport Master Plan Updates are sponsored and funded by the FAA, it is seldom that a study analyzing technology and security systems is approved to utilize federal funds. If the studies are done in parallel, collaboration between the two studies is required to ensure the planning, budgeting, and funding strategies are developed collectively. There are synergies, advantages, and cost savings to an airport when these studies can be developed together. Following this process could improve federal funding approval for larger projects.

The Recommendation Project Analysis Summary (shown in Table 7) provides a template to showcase each recommended project in a one-page summary.

Table 7. Recommended Project Analysis Summary Table

Recommendation Title Project Analysis Summary		
Key Elements of Recommended Project		
Key Drivers for Recommended Project/Initiative		
Project Benefits		
Risk of not Addressing		
Financial Opportunities		
Supporting Project Requirements		
Project Prerequisites?		
Relative Impact of Implementing Project/Initiative		
DESCRIPTION	**MONTHS**	**ROM ESTIMATE**
Planning Services		
Design Services		
Construction Admin		
Implementation *		
TOTAL		
Estimated O&M costs		
Staff Impact	(Document the number of FTE staff positions or indicate “No Staff Impact”)	
Project/Initiative Priority Overview		
Priority	High / Medium / Low (select)	
Basis of Priority		

Recommendation Title Project Analysis Summary
*State implementation basis such as, "Includes power and communications"

This section will explore the differences between ROM costs and an opinion of probable cost. The differences include timing of use and level of detail involved for individual and integrated project types. This is particularly useful when aligning the roadmap to the capital project outlay over the course of several years, which is especially important when establishing a recommended spend plan for the proposed projects.

Additionally, this section will set guidelines using the Project Management Institute's standard methodologies for prioritizing projects, including finding correlations between projects, scheduling, and creating the funding roadmap.

In support of this process, results of airports surveyed show security initiatives are approved based on qualitative as opposed to quantitative factors, such as:

- Benefits in perception (as opposed to hard cost savings)
- Reliability challenges of maintaining older, antiquated technologies
- Mitigating potential threats, saving lives
- Keeping up with supported systems

Examples of security initiative ROM cost estimates that were provided within the survey results from small to large hub airports include:

- Exit Lane Monitoring and Control – $1.5M to $2M
- Perimeter Intrusion Detection System – $8M to $10M
- CCTV Expansion (to terminal buildings and campus) – $4.5M to $5M
- ID Management System – $1.5M to $2M
- CCTV – over $1M
- Security Training Video – $20k to $50k
- New Emergency Operations Center and Airport Operations Center – $500k to $1M
- Patrol Rifles – $20k to $30k
- Perimeter Fencing – $800k to $1M
- Camera Upgrade – $400k to $1M

Once the SMPT has identified recommended projects through the project analysis one-page summary, a roadmap of recommendations can be developed. An example 6-year project roadmap is available in Appendix I.

7.5 Funding Security Initiatives

Airports are required by the federal government to be as self-sustaining as possible and receive little or no taxpayer support. This link from Airports Council International – North America discusses infrastructure funding: https://airportscouncil.org/advocacy/airport-infrastructure-funding. Funding mechanisms are vitally important to achieving the growth and strategic initiatives of an airport. Both aeronautical and non-aeronautical revenue streams can be used by airports; however, both come with certain restrictions. Table 8 provides a quick reference on these revenue sources:

Table 8. Traditional Revenue Sources

Aeronautical Revenue Sources	Non-Aeronautical Revenue Sources
Airline Rents	Concessions
Usage Fees	Parking
Rates and Charges	Airport Access
	Rental Car Operations
	Land Rents
	Advertising

Additionally, some airports have non-traditional revenue streams that can supplement aeronautical and non-aeronautical revenues. Table 9 provides a quick reference on these revenue sources.

Table 9. Non-Traditional Revenue Sources

Non-Traditional Revenue Streams
Passenger Facility Charge and Customer Facility Charge
Science, Technology, Engineering, and Math Education
Electric Ground Vehicle Support
Excess Bond Proceeds
Alternative Fuel Uses
Renewable Energy
Commercial Space Rental
Executive Office Space Rental
(https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=4224&context=roadschool)

The prioritized roadmap described in the previous section can be used to assist airports in making informed decisions on potential funding strategies for aspects of their SMP and related security initiatives. An example of a roadmap can be found in Appendix I. It begins with an examination of the type of justification (e.g., ROI, Business Case, etc.) that can be performed to articulate the need for the security initiative, and then explores the type, purpose, and broad eligibility criteria of various federal, state, local, and other alternative funding sources and mechanisms that may be available to the airport owner-operator. In many cases, security initiatives are funded as part of larger project (e.g., overall terminal improvements) and their justification for funding is embedded in that of the larger project.

Input on the justifications used for security-related projects comes primarily from the surveyed airport participants who provided feedback on the nature and type of analysis required to support their security initiative decision-making. Guidance on funding mechanisms is also based on survey participant input, coupled with research and analysis of publicly available literature on grant programs and other potential funding sources at the federal, state, and local levels.

7.5.1 Federal Funding and the AIP

The federal funding process typically begins with an airport's 10-year Airport Capital Improvement Plan, which identifies and prioritizes projects for an airport, including those related to security. These plans usually need to be submitted to the appropriate agencies prior to the beginning of each fiscal year when external funds are desired.

Recognizing the public good provided by airports and air transportation, Congress created the AIP to provide funding for safety, capacity, security, and environmental projects at the nation's airports. Congress has had various airport grant programs since WWII; the AIP in its current version was created in 1982 under the Airport and Airway Improvement Act and disburses funds to airports through a combination of entitlement and discretionary programs. The AIP's entitlements are further broken down into four distinct components:

1. **Primary Airports Entitlements**: Primary airports (large- or medium-hub) receive entitlements based on a per-passenger formula; this number is reduced if the airport charges a Passenger Facility Charge; primary airports receive a minimum of $1 million and are capped at $26 million.
2. **Cargo Entitlements**: FAA distributes 3.5% of the AIP to qualifying cargo airports based on their share of total cargo handled.
3. **State/GA Apportionments**: 20% of the AIP is distributed to non-primary—including GA—airports; these airports receive 1/5 of their 5-year development estimate, capped at $150,000. The remainder is distributed to the states, based on an area/population format.
4. **Alaska Supplemental Funds**: Congress apportions funds to certain Alaskan airports to ensure they receive no less than they did under previous legislation in 1980.

> A large-hub airport surveyed, for example, received some AIP funding for the bollards along all the curbs and some critical infrastructure for hardening perimeters. The rest of the funding came from CIP funds.

After the entitlement funding is complete, what remains constitutes the discretionary fund, which the FAA can distribute more freely. Certain categories of projects receive a minimum funding level using set-asides:

- **Noise:** An amount equal to or greater than 35% of the discretionary fund must be spent on noise-related projects; if entitlement funds are used for noise projects, it counts against the set-aside.
- **Military Airports:** 4% of the discretionary fund is used to help convert former military airports to civilian use.
- **Reliever:** 2/3 of 1% of AIP is reserved for grants to operators of airports designated as relievers by the DOT Secretary.
- **Capacity/Safety/Security/Noise:** Of the remaining discretionary funds, 75% must be used for projects that address one or more of these issues.
- **Remainder:** The remaining 25% of the discretionary fund constitutes "true discretionary" funding, which FAA can distribute to any eligible project at any National Plan of Integrated Airport Systems airport.

The airport owner/operator must provide a local match for AIP-funded projects. This ranges from 5%–25% based on the project type and airport size, and could comprise PFCs, local revenues, or other funds for this local match.

FAA coordinates closely with TSA on assessing the merits of security-related projects. While perimeter fencing, or ACSs may be deemed AIP-eligible, terminal or baggage system reconfiguration needed to install bulk explosive detection systems are typically ***not*** eligible.

In general, safety and security projects include development that is required by federal regulation, airport certification procedures, or design standards, and are intended primarily for the protection of human life. AIP-eligible security projects may be security fencing, access control from aircraft movement areas to the terminal, and other security enhancements required by the title 14 CFR § 1542 regulation. AIP funding for security development currently totals approximately $475 million, a decrease of $280 million from the last report. Primary airports have identified ACSs and other security improvement projects totaling $148 million (31%); Non-Primary airports have identified approximately $327 million (68%), with the majority related to perimeter fencing.

To be eligible for AIP funding, security-related projects or equipment must be identified in the airport's TSA-approved ASP, SDs, or other emergency requirement. Furthermore:

- ACSs are generally eligible, as are projects to prevent unauthorized access to the AOA, such as fingerprinting equipment, computerized door controls, perimeter fencing, and CCTV monitoring for the AOA.
- Additionally, any application for a project that would require operations or maintenance from TSA staff must include TSA's commitment to provide it.
- FAA may also approve funding for security projects on other facilities on the airport if additional justification is submitted.
- Equipment used by TSA for the screening of passengers is ineligible, but structural changes to the screening checkpoint area to accommodate new equipment required by TSA are generally eligible.

Projects included in the safety category include obstruction lighting, obstruction removal, acquisition of ARFF equipment required by Part 139, construction or expansion of ARFF buildings, and improvements to Runway Safety Areas. Safety development funding currently approximates $1 billion, a decrease of $137 million from the last report, largely reflecting the fact that many significant Runway Safety Area improvements have now been funded and implemented. The 382 primary airports account for 77% of the safety projects, with non-hub airports accounting for 30%.

Both categories—safety and security—account for about 5% ($1.5 billion) of the overall amount funded by AIP. The FAA continues to give safety and security development the highest priority to ensure rapid implementation and to achieve the highest possible levels of safety and security across US airports.

In surveys of airports, respondents identified several projects—an airfield security wireless project and multiple security system upgrades—that have been funded by the FAA's AIP program.

7.5.2 Federal Funding and the TSA

The TSA's Advanced Surveillance Program improves the security of US transportation infrastructure by promoting enhanced surveillance capabilities (e.g., CCTV) and providing industry partners and agencies with expertise and knowledge related to surveillance methods that are effective and suitable. The program also provides funding to transportation facility operators for enhanced surveillance infrastructure and capabilities to support TSA requirements for security of critical areas.

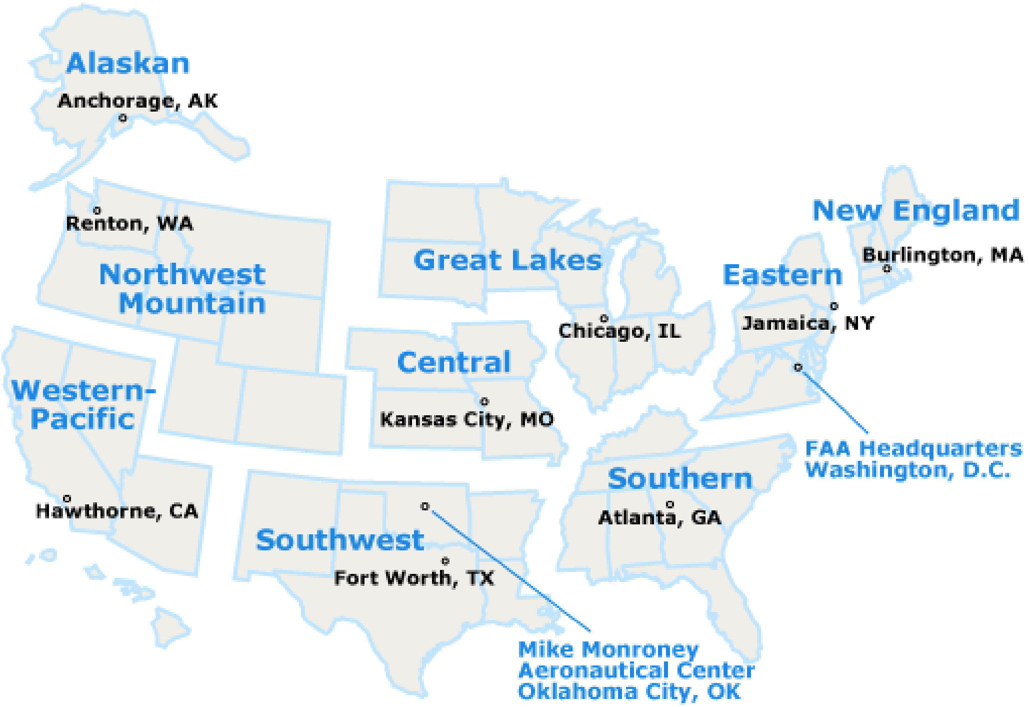
The overall purpose of these surveillance systems is to provide TSA staff and their airport partners with clear, detailed, real-time images of critical areas to cover security incidents and support resolution of liability claims[2].

Additionally, the TSA's Law Enforcement Officer (LEO) Reimbursement Program strives to maximize the mutual benefits of the program through consolidated efforts with airport stakeholders, industry partners, and TSA stakeholders to fulfill the common goal of ensuring the safety of the traveling public. The LEO Reimbursement Program is part of the joint efforts between TSA and airport operators nationwide to deploy enough LEOs in support of passenger screening activities at the checkpoint to meet the dual responsibilities of ensuring passenger safety, and countering risks to transportation security pursuant to 49 USC § 44903(c) and 49 CFR § 1542. Eligibility is limited to FAA § 139 Airport Certificate holders that have incurred LEO service costs due to post-September 11 security mandates.

7.5.3 State/Local Funding for Security Initiatives

Many states as well as local entities (e.g., cities, regional planning agencies, etc.) have developed programs to assist airport owner/operators with funding security-related projects. The intent of this information is to give an example of what may be found regionally and/or by individual states. Funding sources are continually changing, so airports are encouraged to research their specific state and region annually to see what sources might be available. These programs vary dramatically by state and examples are summarized in Appendix G. A few detailed examples are shown in Figure 9 and described in the sections that follow.

Figure 9. Regional/State FAA Funding Map



Source: https://www.faa.gov/about/office_org/headquarters_offices/arc

[2] For more information on TSA's Advanced Surveillance Program, go to : https://www.sskies.org/images/uploads/subpage/Checkpoint_TSA_BASELINE_VIDEO_SURVEILLANCE_FUNCTIONAL_REQUIREMENTS_V1.1.pdf

7.5.3.1 Eastern States Examples

In Virginia, a key element to the strength, security, and continued growth of the state's aviation system is the partnering between the Virginia Aviation Board (VAB), Virginia Department of Aviation (DOA), FAA, and airport sponsors. Each has roles and responsibilities that support individual airports and the statewide air transportation system:

- VAB – The VAB establishes financial assistance programs and allocates funds for CIPs. The VAB sets policies to guide the funding programs and to promote and develop safe and secure aviation practices and operations in Virginia. The VAB hears airport sponsor and citizen concerns on matters pertaining to aviation, and acts as a liaison to the department in order to be responsive to local jurisdictions, users of the system, and citizens. Airport sponsors are encouraged to maintain regular contact with their representative VAB members, keeping them aware of issues affecting the operations and planned development of their airports.
- Virginia DOA – The Virginia DOA provides financial and technical assistance to eligible airport sponsors for the planning, development, promotion, construction, and operation of airports and aviation facilities. DOA also administers applicable provisions of the Code of Virginia, plans for the development of the state aviation system, licenses airports and aircraft, and promotes aviation activities within the state.
- FAA – The FAA provides financial and technical assistance to eligible airport sponsors for the planning, design, and construction of airports and aviation facilities. FAA also sets design and operation standards for airports.
- Virginia Airport Sponsors – An airport sponsor has many obligations to its airport, ranging from financial dealings and long-term development planning to daily maintenance and operational activities. A sponsor is solely responsible for ensuring that the airport is compliant with federal and state grant assurances, board policies, and various licensing and design criteria.

An example of the state's funding of security-related initiatives is the Voluntary Security Program (VSP), which is focused on enhancing the security of public-use GA airports in Virginia. The VAB has delegated the authority to review and approve funding requests for the VSP to the Virginia DOA.

Before a GA airport sponsor can receive funding for a security improvement project, the airport must first be declared a Secure Virginia Airport as described in the state's GA Airport Voluntary Security Certification Program. In addition, a security improvement project must be identified on the sponsor's approved airport security plan to be eligible for state funding. VSP does not have prerequisites for projects to conduct security audits and develop security plans. The following are examples of eligible for VSP funding:

- Airport security audit
- Airport security plan
- Terminal area fencing, including 500 feet of vinyl-coated fence
- Perimeter fencing
- Electronically controlled entry gates
- External and internal surveillance systems
- Security signage
- Security lighting
- Security barriers

A fence-clearing project is eligible one time only. The continued maintenance of the terminal area and perimeter fence lines is a sponsor's responsibility. Operational costs, such as the hiring of security guards, are not eligible.

VSP funds 100% of projects to conduct security audits and develop security plans. The program funds 90% of the design and installation of security improvements that address deficiencies identified in plans and audits.

Virginia DOA will review security audits and plans, and it will review and approve engineering agreements, plans, and specifications for security improvements.

When funds are not available under the VSP, a sponsor may submit project requests under the Airport Capital Program for consideration by the VAB. The projects must meet the eligibility requirements of the VSP, and the required supporting documents for the Airport Capital Program must be provided as part of the project request submission.

The Maryland Aviation Administration has a statewide Aviation Grant Program that offers financial assistance to public owned, public-use airports. These Special Grants are available for airport projects—including security—that are either non-AIP eligible or are AIP eligible but not AIP funded. Projects that are non-revenue generating and considered reasonable for the improvement, development, and/or preservation of the airport are eligible for Special Grant funds. The Special Grant Program is not intended for the development of new landing facilities, and annual funding is typically limited. Special Grant funding is set at 75% of state participation of eligible cost and is a reimbursement program. Due to the limits on funding, Special Grant requests should be scoped for completion within the same fiscal year.

Security-related projects (e.g., access control to AOA; airside security improvements, etc.) have a relatively high priority on the state's criteria rating system, and often require the existence of an ASP.

7.5.3.2 Southern State Example

Florida law allows Florida's DOT (FDOT) to fund any capital project on airport property and any services that lead to capital projects, such as planning and design services. The only off-airport projects allowed are the purchase of mitigation lands and aviation easements, noise mitigation, and access projects for intercontinental airports. Airport capital equipment is eligible for funding if it is not too closely related to day-to-day operations. In general, operational costs such as maintenance services, equipment, and supplies are not eligible for aviation grants.

To be eligible for the Florida Aviation Grant Program, airport projects must be consistent with the airport's role defined in the Florida Aviation System Plan and, to the maximum extent feasible, with the approved local government comprehensive plan. In addition, capital projects must be part of an FDOT-approved airport master plan and/or airport layout plan, have an airport sponsor (local government), be identified in the FAA's AIP, and be entered into the FDOT Aviation database via the Joint Automated Capital Improvement Program.

The Florida Aviation Grant Program includes funding for security projects such as lighting, signage, fencing, baggage checkpoint improvements, access control, facility hardening, plans, etc. FDOT provides up to one-half of the local share of commercial service airport project costs when federal funding is available. For example, FDOT provides up to 12.5% of project costs when the FAA provides 75% of the funding. Using this example, if a project cost equaled $100,000, the FAA would provide

$75,000, FDOT would provide $12,500, and the local share would be $12,500. When no federal funding is available, FDOT provides up to 50% of the total project costs.

For GA airports, FDOT provides up to 80% of the local share of GA airport project costs when federal funding is available. For example, FDOT provides up to 8% of project costs when the FAA provides 90% of the funding. Using this example, if a project cost equaled $100,000, the FAA would provide $90,000, FDOT would provide $8,000, and the local share would be $2,000. When no federal funding is available, FDOT provides up to 80% of the total project costs

Other funding mechanisms that may be applicable to security-related projects in Florida include the following:

- The State Infrastructure Bank is a revolving loan and credit enhancement program consisting of two separate accounts: a federally funded account and a state-funded account. This program operates like a bond in that it is used where a dedicated revenue stream is present.
- The federally funded account is capitalized by federal money matched with state money, as required by law under the Transportation Equity Act for the 21st Century. All repayments are repaid to the federally funded State Infrastructure Bank account and revolved for future loans. Projects must be eligible for assistance under title 23, US Code or capital projects as defined in Section 5302 or title 49, US Code. Projects must be included in the adopted comprehensive plans of the applicable Metropolitan Planning Organization (MPO) and must conform to all federal and state laws, rules, and standards.
- The state-funded account is capitalized by state money and bond proceeds. All repayments are repaid to the State Board of Administration where debt service is paid on any outstanding bonds with the remainder returned to the state-funded account and revolved for future loans. Projects must be consistent, to the maximum extent feasible, with local MPO and local government comprehensive plans and must conform to policies and procedures within applicable Florida Statutes and other appropriate state standards for the transportation system.
- The Transportation Regional Incentive Program (TRIP) was created to encourage regional planning by providing state matching funds for improvements to regionally significant transportation facilities identified and prioritized by regional partners. The following entities are eligible to participate in the TRIP program: two or more contiguous MPOs; one or more MPOs and one or more contiguous counties that are not members of an MPO; a multi-county regional transportation authority created by or pursuant to law; two or more contiguous counties that are not members of an MPO; MPOs composed of three or more counties.

TRIP funds are to be used to match local or regional funds up to 50% of the total project costs for public transportation projects. In-kind matches such as right-of-way donations and private funds made available to the regional partners are also allowed. Federal funds allocated for urbanized areas with a population over 200,000 may also be used for the local/regional match.

7.5.4 Cost and Funding Considerations

Input from survey participants and site visits provided several helpful insights that airport owner-operators should consider when developing cost estimates, justifications, and funding strategies for their security initiatives, such as:

- The way an airport plans to budget and schedule project items may determine if parts of the project end up not being funded; for example, as an airport nears the end of a project and money has been spent on unexpected issues, some final items may not be able to be funded if the true costs have not been properly calculated up front. An example of a ROM Costing Summary Table can be found in Appendix H.

- The security department is not typically heavily involved in AMP efforts, as their project timelines are usually much shorter than those of the AMP; however, where it is possible to obtain more AIP funding by having security projects incorporated into the AMP, this coordination should be encouraged.
- One surveyed airport changed the name of the AMP to "Capacity Enhancement Plan," and as the result of staff turnover, many current personnel do not know the history of the renaming and its relevance to related documents like the Security and IT Master Plans. The airport's resulting planning approach seems to be more finance-driven as opposed to operationally focused.
- Getting early involvement of TSA and/or FAA in security project conversations can help get reimbursement agreements in place sooner in the project lifecycle. It is recommended that annual coordination occurs even if it is merely to exchange information and provide updates.
- The relationship of the SMP to the AMP should be clarified in the roadmap section, found in Section 7.4 and Appendix I, by discussing improvements that have been accepted by senior management along with their associated costing; airports need to be careful that nothing labeled SSI gets into the AMP.
- For airports that are part of a city or county (e.g., an Aviation Department), some security initiatives (e.g., radio systems, police dispatch, and 911 capabilities) may be eligible for funding as part of a broader, city/county-wide, security-related effort.
- AMPs are not updated as quickly as technology infrastructure changes; software requirements need to be updated even more frequently.
- Roadmap and costing need to include all costing. In some instances, the airport road-mapped projects and made a case for them in the gap analysis. They were able to get funding for each of the road-mapped projects in order of priority; however, when uncalculated costs emerged, some of the lower priority projects had no funding left. Therefore, costs that are typically uncalculated, such as operations and maintenance fees, should be included in costing.
- Airports need to make sure the true capital cost needs for implementation and maintenance are included; sometimes overall project costs can be saved by improved maintenance practices, which defer or eliminate the need for earlier replacement.
- Tenant lease agreements (both airline and concessionaire) and rates/charges calculations can directly or indirectly help fund security enhancements. Some methods include modifying lease requirements, incorporating security enhancements into developer agreements, adding security costs to the rate base, or recouping via fees.

SECTION 8: MONITORING AND MAINTENANCE PHASE

The SMP should be considered a living document, which requires a periodic and systematic refresh. This section provides guidance on refreshing the SMP once it has been formally adopted by the airport. Areas of focus will include identifying the frequency of updates, key stakeholders, and maintainers of the document, and putting governance in place to support the strategic direction of the projects put into the capital plan because of SMP recommendations.

One approach may be to periodically update the SMP based on the project roadmap. A review of the SMP should be conducted annually to ascertain currently funded projects and their status, and to identify projects to be funded next. If this activity is done as part of project management, the task of maintaining the roadmap and funding will be less challenging. This process will also help the airport to understand when a roadmap is nearing completion and the next project roadmap and funding process needs to begin.

8.1 Governance

The most comprehensive way to maintain the SMP is through documented business processes and a Governance structure. Aligning a group of individuals made up from various key stakeholder departments to oversee the maintenance of the plan can ensure continual visibility and awareness. A Governance document should include the following at a minimum:

- Formal direction
- Formal accountability
- Budget planning
- New standards and policies
- Continual upgrade and maintenance
- Planning for funding future security systems and resources

Governance should also include external stakeholders, such as tenants and mutual aid partners. Fostering a communicate-and-educate philosophy with such entities is considered proactive and a best practice.

8.1.1 Operational/Technical

Operational and technical planning is also important. Governance efforts through an established committee should also have representation by the daily managers, key tenants, and users of security technology systems, networks, and resources.

8.2 Security Rules and Regulations

Industry best practices, and federal and local airport rules and regulations must be consistently reviewed, updated, and maintained. As these security rules and regulations change, communication and coordination with internal and external stakeholders must be effectively facilitated by the airport security department and staff. These changes may impact the way a tenant operates and conducts business, or necessitate alterations to lease language between the airport and a tenant. It is recommended that changes affecting security rules and regulations at an airport go through the properly established Governance process. The reason for this recommendation is the group or body that oversees Governance can help to support the changes, analyze the impacts, make recommendations on how to implement the changes, and be a conduit for communication and enforcement throughout the airport community.

8.3 Lifecycle Replacement of Assets

It is important to look at the lifecycle of all assets, not just technology. All lifecycle costs must be realized so an airport does not invest in an expensive technology system when the hardened infrastructure is failing. For example, if an expensive PIDS or ACS is planned for an airport fence line, but the fence infrastructure itself is failing and the fence material and installation was not part of the total project, then costing will cause negative budgetary impacts. In this case, the replacement of the fence should also be included in the planning process. This also helps an airport build a better Business Case. This section briefly describes the asset types covered under lifecycle replacement and best practices through Asset Lifecycle Management (ALM).

> A large-hub airport surveyed believes strongly in the lifecycle replacement of assets. Their process includes the comparison of costs over the lifecycle for new design and installation versus lifecycle of the existing systems/infrastructure, including maintenance for both options. This helps them to make the case for future capital investment and supporting maintenance.

8.3.1 Asset Types

Lifecycle replacement through ALM, as a strategic planning effort, can cover all equipment comprising the security systems at an airport, such as described in the following sections.

8.3.1.1 Operational Technology Assets

These assets include Supervisory Control and Data Acquisition, Human-Machine Interfaces, and Programmable Logic Controller equipment.

- Gate controllers
- Door controllers
- Camera controllers
- Heating and air controllers
- Video cameras
- Door security hardware

8.3.1.2 IT Assets

IT assets are systems for storing, retrieving, and sending information.

- Software
- Hardware such as servers, computers, and switches
- Network infrastructure
- Cloud-based infrastructure

8.3.1.3 Internet of Things (IoT) Assets

IoT refers to the network of physical objects made smart with electronics, sensors, software, and network connectivity.

- Request to exit, gate (motion) sensors
- Heating and air (temperature) sensors
- Passive infrared motion detectors
- Glass break detectors
- Ultrasonic/infrared detectors
- Magnetic switches
- Gas sensor

8.3.1.4 Data and Information Assets

These assets refer to the data and information that resides in security systems. Often, for example, the ID badging and credentialing system will store SSI such as codes to open security gates or airport as-built drawings, and personally identifiable information such as a person’s name, social security number, and/or driver’s license number.

- Databases
- Sensitive files and folders
- Password-protected network drives

8.3.1.5 Physical Security Assets

These physical items are used to protect personnel, hardware, software, networks, and data from physical actions and events (e.g., natural disasters, fire, flood, burglary, theft, vandalism, and terrorism).

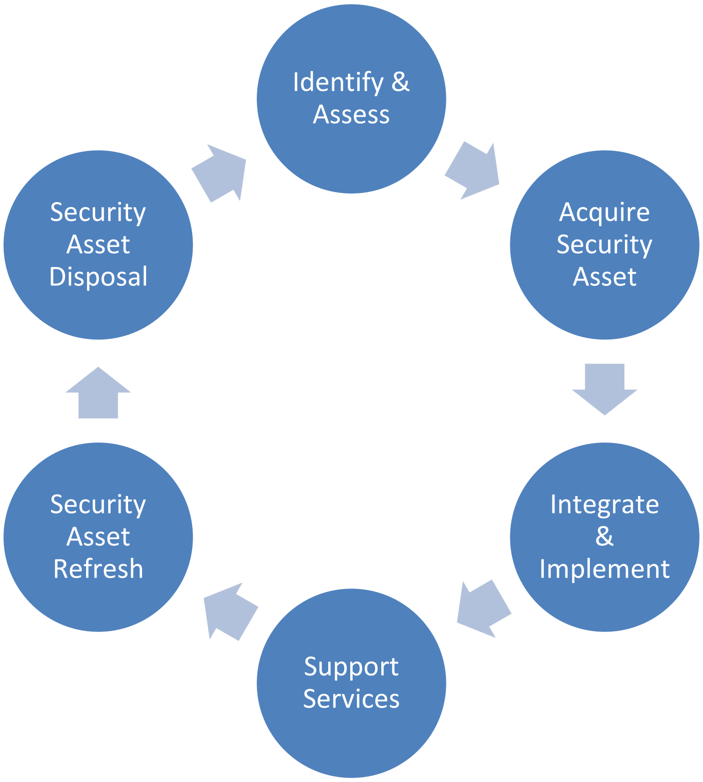
- Gates
- Fences
- Doors
- Bollards
- Buildings

8.3.2 Asset Lifecycle Management

Defining a lifecycle replacement plan is a very important aspect of SMP. ALM is a multi-phased approach that encompasses the planning, design, acquisition, implementation, management, and disposal of all the elements comprising the security infrastructure. Using an ALM approach will include all asset types described in the previous sections (see Figure 10).

Following industry best practices, ALM strives to ensure that a wide-range of Key Performance Indicators, including safety, compliance, quality, and operating costs are met, while also providing a framework for an airport to manage their security system’s assets over time.

Figure 10. Asset Lifecycle Management



8.3.2.1 Identify and Assess Phase

This phase involves requirements analysis and technical needs, and covers the following areas:

- Acquisition strategy
- Financial plans aligned with budget availability
- Plan for ongoing support
- Project Management Plan
- Project implementation plan
- Asset tracking and retirement/disposal strategy

(Reference: https://www.unicomgov.com/files/4914/9994/9798/UGI_TLM_WhitePaper.pdf)

8.3.2.2 Security Asset Acquisition Phase

This phase involves obtaining assets and services during the execution of the previous phase. This process needs to be documented, and the document maintained through regular updates, at least quarterly. Maintaining the document will help reduce future efforts.

8.3.2.3 Integrate and Implement Phase

This phase follows a detailed plan that maximizes efficiencies by providing important information on security assets, such as:

- System configurations
- Asset management

- Quality assurance
- Onsite and/or remote engineering
- Project management

8.3.2.4 Support Services Phase

The support services phase includes post-implementation support services. These services, such as ongoing proactive maintenance are critical to monitor and manage to keep security systems and assets performing in their optimal state. The airport department or group who manages these services (or, in some cases, provides these services) is responsible for:

- Configuration and change management, technology restorations, and software upgrades
- Maintenance agreements and SLAs
- Warranties
- Ongoing collaboration between the airport and the vendors
- Periodic reviews and performance metrics designed to support the SLAs in place

8.3.2.5 Security Asset Refresh Phase

The security asset refresh phase includes a plan to allocate funding for refreshing all assets that support security systems and services. This enables the airport to upgrade and keep up with increasing user demands, including support to prevent system failures and service interruptions. Refresh strategies are driven by:

- Business objectives
- Security initiatives
- Financial requirements
- Growth requirements

8.3.2.6 Security Asset Disposal Phase

The security asset disposal phase includes a plan to retire assets through multiple options such as cascading to administrative or other business units (e.g., moving older video surveillance cameras to areas that are not critical, but essential to situational awareness) or disposing of the equipment responsibly.

Special attention should be given to securing data and information during the disposal process. For example, disk drives will need to be either erased or physically destroyed. Or, if an asset is redeployed elsewhere, a new standard image should be deployed prior to moving.

SECTION 9: CONCLUSION

This guidebook has been configured to help airports develop a methodical approach to creating and maintaining an SMP. Many airports may have already engaged in some of the tasks needed to prepare an SMP, such as the gathering of existing conditions data, and/or the preparation of a threat and vulnerability assessment. Other airports have a sense of their needs and requirements but may not have formally documented them. Airports are encouraged to start with what has already been documented in order to begin to lay the foundation of their SMPs.

Starting an SMP effort may seem like a daunting undertaking. Most airports manage and balance several projects every year. The SMP should be considered in a similar way to any other planning project. To that end, it may be useful to understand what the final product might look like in order to start the SMP effort. The recommendation and road mapping paragraph in Section 7.4 may be a good place to start. Airports can also review a roadmap example such as the one shown in Appendix I to get a sense of the end product, so that they can begin to determine if outside support or resources are needed, and when in the overall SMP process to bring in those resources.

External resource(s) may be a good alternative for augmenting already busy workloads. The SMPT could work with a project manager who is experienced in developing SMPs. Committing funds to the process early on may ensure better buy-in with staff and executive management to move forward with developing an SMP. As with any planning project, airport planners can expect a lot of interaction amongst different diverse airport stakeholders, staff, and departments. Besides the benefits highlighted within this guidance, an SMP can also be a great tool to help create and bridge relationships between security, operations, maintenance, finance, and planning departments, along with airlines and federal agencies.

REFERENCES

Airports Council International. *Airport Infrastructure Funding.* https://airportscouncil.org/advocacy/airport-infrastructure-funding

ASIS Online. 2013. *Security Business Case Development Guide.* https://sm.asisonline.org/ASIS%20SM%20Documents/SecurityBusinessCaseDevelopmentGuide.pdf

Department of Homeland Security. 2015. *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide.* https://www.dhs.gov/sites/default/files/publications/isc-planning-managing-physical-security-resources-dec-2015-508.pdf

Federal Aviation Administration. *Regions and Property Operations.* https://www.faa.gov/about/office_org/headquarters_offices/arc

Giles, Timothy D. *How to Develop and Implement a Security Master Plan.* Boca Raton: Auerbach-CRC Press, 2008.

Government Publishing Office. *TSA 49 CFR Part 1520, Security Rules for All Modes of Transportation*. https://www.govinfo.gov/content/pkg/CFR-2011-title49-vol9/pdf/CFR-2011-title49-vol9-part1520.pdf

Government Publishing Office. *TSA 49 CFR Part 1542, Airport Security*. https://www.govinfo.gov/content/pkg/CFR-2010-title49-vol9/pdf/CFR-2010-title49-vol9-part1542.pdf

Government Publishing Office. TSA, Information Publication A-001, Version 2. July 2017. *Security Guidelines for General Aviation Airport Operators and Users*. https://www.tsa.gov/sites/default/files/2017_ga_security_guidelines.pdf

iSixSigma. *Pugh Matrix.* https://www.isixsigma.com/dictionary/pugh-matrix/

National Institute of Standards and Technology. 2017. *An Introduction to Information Security* https://www.nist.gov/fusion-search?s=800-12&commit=Search

National Safe Skies Alliance. 2014. *PARAS 0004 - Recommended Security Guidelines for Airport Planning, Design, and Construction.* https://www.sskies.org/images/uploads/subpage/PARAS_0004.Recommended_Security_Guidelines.FinalReport.v2.pdf

———. 2017. *PARAS 0010 - Guidance for Protecting Access to Vital Systems Impacting Airport Security.* https://www.sskies.org/images/uploads/subpage/PARAS_0010.SecuritySystemsAccess.FinalReport.pdf

———. 2018. *PARAS 0014 - Blast Mitigation Strategies for Non-Secure Areas at Airports.* https://www.sskies.org/images/uploads/subpage/PARAS_0014.BlastMitigationStrategies.FinalGuidebook.pdf

Purdue University, School of Aviation and Transportation Technology. 2018. *General Aviation Airports: Innovative Revenue Strategies.* https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=4224&context=roadschool

Radio Technical Commission for Aeronautics. 2018. *DO-230I - Standards for Airport Security Access Control Systems*. https://my.rtca.org/NC__Product?id=a1B36000007GSznEAG

Security Management. 2018. *Starting* From the End: Creating a Master Security Plan. https://sm.asisonline.org/Pages/Starting-from-the-End---Creating-a-Master-Security-Plan.aspx

Simplicable. 2017. *9 Types of Design Constraint.* https://simplicable.com/new/design-constraints - Design Constraints, Simplicable

Transportation Security Administration. *TSA Baseline Video Surveillance Functional Requirements – Checkpoint.* https://www.sskies.org/images/uploads/subpage/Checkpoint_TSA_BASELINE_VIDEO_SURVEILLANCE_FUNCTIONAL_REQUIREMENTS_V1.1.pdf

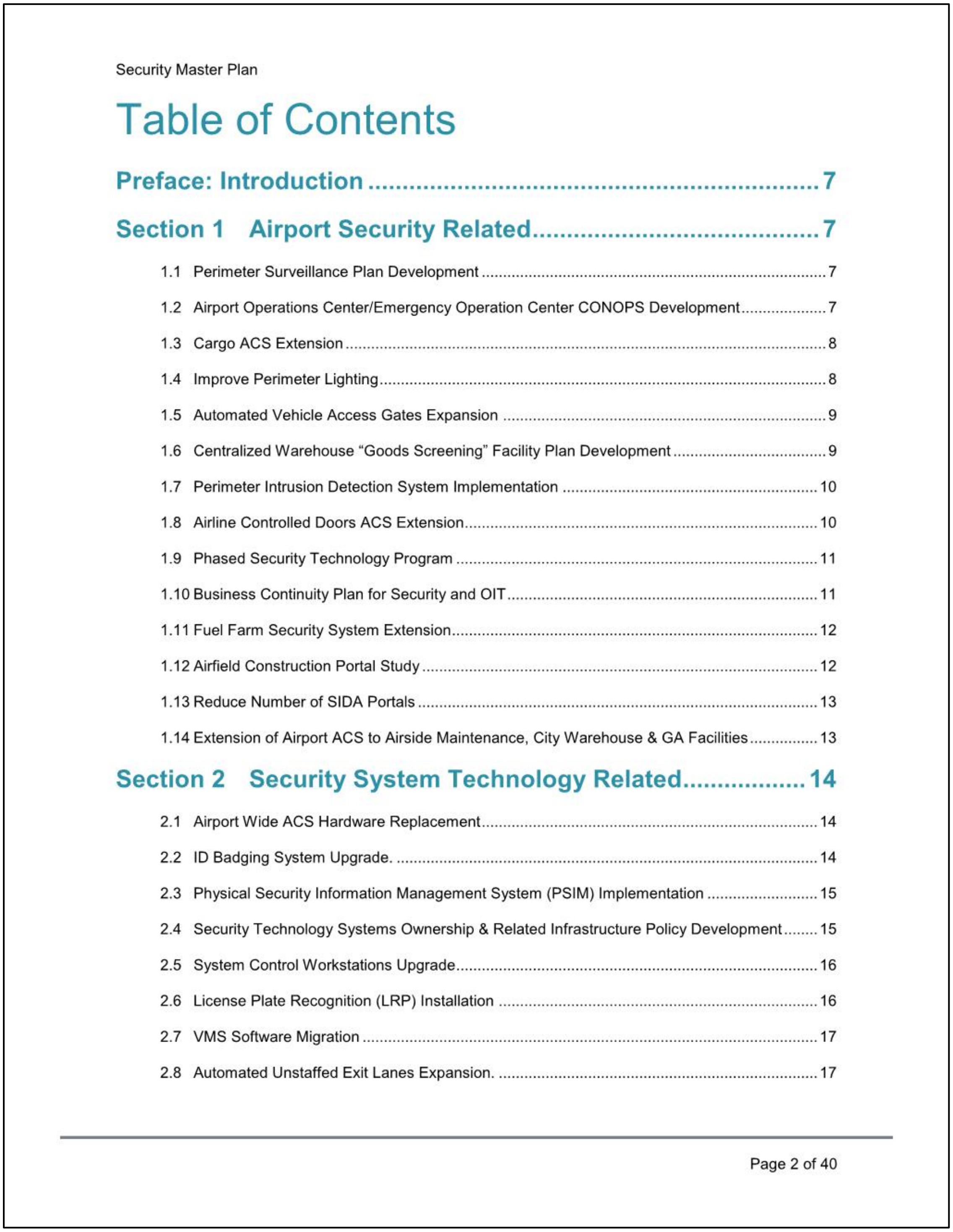
UNICOM Government, Inc. 2018. Technology Lifecycle Management. https://www.unicomgov.com/files/4914/9994/9798/UGI_TLM_WhitePaper.pdf

Watts, Stephen. June 21, 2017. *IT Security Vulnerability vs Threat vs Risk: What’s the Difference?* https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/

ABBREVIATIONS, ACRONYMS, & INITIALISMS

ACS	Access Control System
ALM	Asset Lifecycle Management
AMP	Airport Master Plan
ALP	Airport Layout Plan
ASMP	Airport Safety and Maintenance Program
ASP	Airport Security Program
CBP	Customs and Border Protection
CIP	Capital Improvement Plan
DOA	Department of Aviation
FDOT	Florida Department of Transportation
GA	General Aviation
GRF	General Revenue Fund
LEO	Law Enforcement Officer
MPO	Metropolitan Planning Organization
NIST	National Institute of Standards and Technology
PARAS	Program for Applied Research in Airport Security
PIDS	Perimeter Intrusion Detection System
PSIM	Physical Security Information Management
RFQ	Request for Qualifications
ROM	Rough Order of Magnitude
SASP	State Airport System Plan
SMP	Security Master Plan
SMPT	Security Master Plan Team
TRIP	Transportation Regional Incentive Program
TVA	Threat and Vulnerability Assessment
VAB	Virginia Aviation Board
VMS	Video Management System
VSP	Voluntary Security Program
VSS	Video Surveillance System

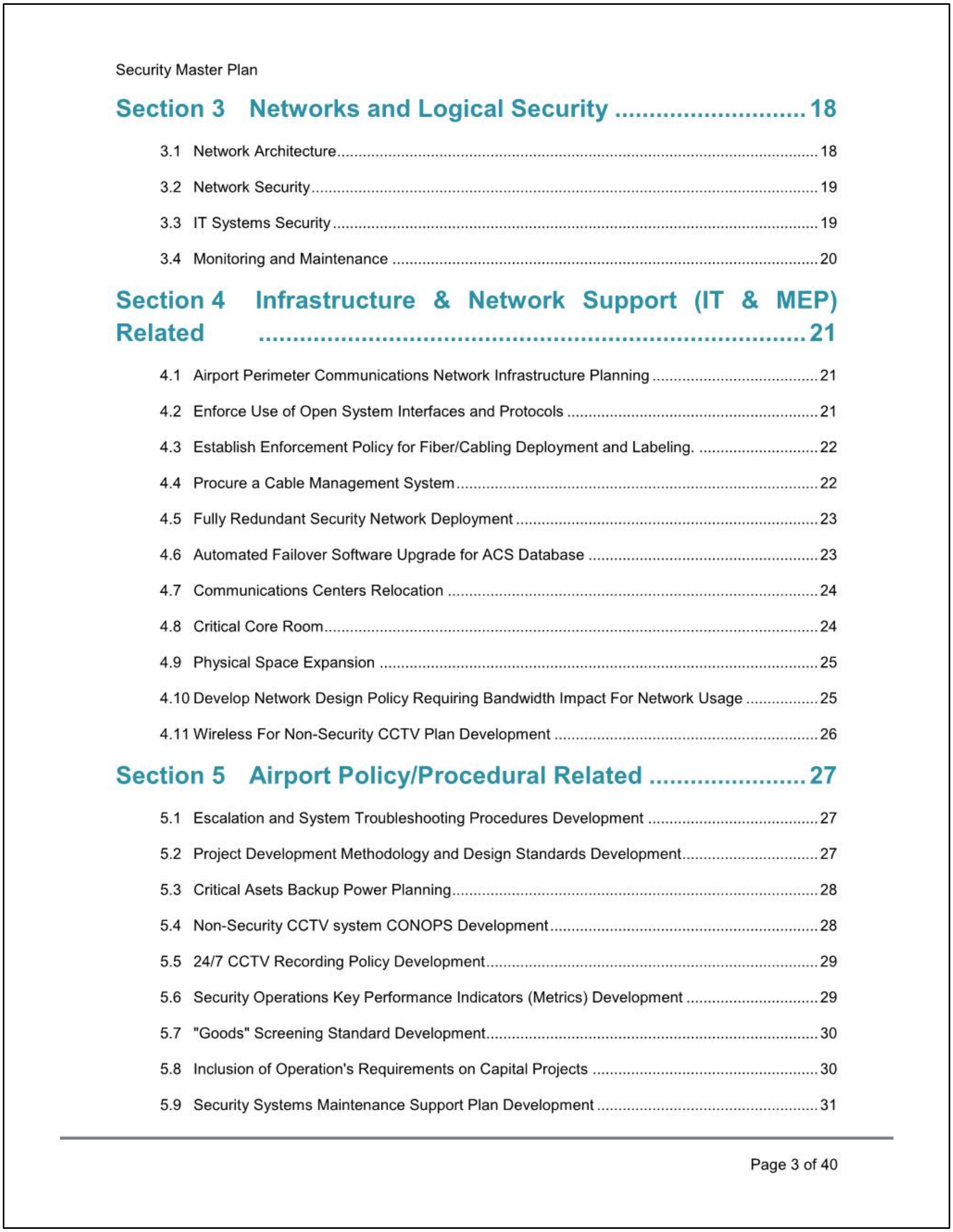
APPENDIX A: SMP CONCEPT OUTLINE FOR ORGANIZATION OF RECOMMENDATION (EXAMPLE)

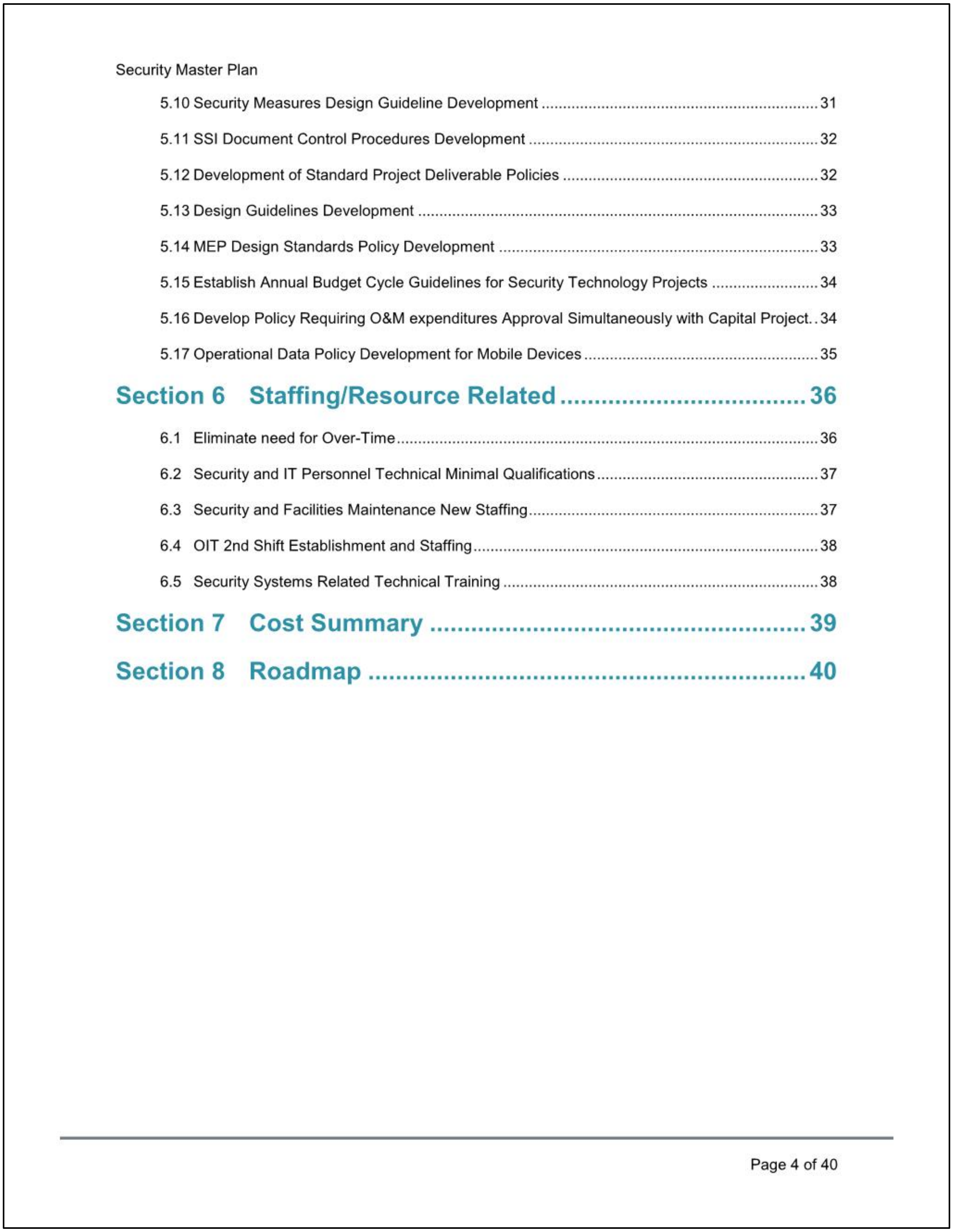


Security Master Plan

Table of Contents

Page 2 of 40





APPENDIX B: BUSINESS CASE / PROJECT CHARTER (EXAMPLE)

BUSINESS CASE

I. Introduction

A. Purpose of Business Case

The introduction describes the purpose of the Business Case. Key questions to answer in the introduction will include:

- How does the current state of aviation security at the airport compare to aviation security at similar airports and potential future aviation security outlook? Are there gaps, weaknesses, and vulnerabilities at the airport?
- What is the status of aviation security at the airport in terms of the systems, operations, processes, procedures, technologies, capabilities, staffing, and ongoing work?
- What is the future of aviation security, based on national, international, and local issues, including changes in technologies, regulatory requirements, airport growth, and operations?
- What is the current state-of-the-art and best practices for aviation security at similar airports?
- What is and what should the aviation security philosophy and strategy be at the airport?

II. General Project Information

Table B-1. General Project Information

Submission Date	<mm/dd/yyyy>
Requested By	<Enter full name>
Business Owner	<Enter Business Owner/Manager supporting this document>
Airport Security Owner	<Enter the Security Owner/Manager supporting this document>
Contact Info.	<Enter email address and phone number of primary contact>
Project Name	<Enter a name for the proposed project>
Desired Start Date	<Enter a desired start date for the requested project>

A. Business Need

Provide an explanation of the business need that the SMP will fulfill. Include expected benefits from the investment of airport resources.

Example: The airport's safety and security are a top priority. Planning for the operational systems, networks, and labor involves multiple stakeholders over the span of many years through lifecycle management. Benefits derived from a healthy security master plan include, but are not limited to, increased awareness, future-proofing against out-of-date equipment, and providing the security needed to maintain efficient operations and meet legal requirements.

B. Airport Security Need

Provide an explanation of the airport security management need that the SMP will fulfill. Include expected benefits from the investment of airport security resources.

C. Goals/Scope

Provide a purpose, scope, and goals of the SMP. Describe short-term, long-term, and operational security goals and objectives.

D. Risks/Issues

Provide business and technical risks/issues of executing and not executing the SMP project. Risk areas may include initial costs, lifecycle costs, technical obsolescence, reliability of current systems, dependencies, future procurements in the CIP, external influences (e.g., airlines and other tenant security initiatives), airport change management, privacy of existing and future information, and project resources.

III. High Level Business Impact

Provide a high-level business impact description for implementing an SMP. This can include plans for addressing ongoing security operations and future growth, and detail how these areas will be managed. Consider requirements for additional services, security hardware and software, building materials, and space, and provide an idea of how funding will be approached.

IV. Alternatives and Analysis

A. Alternative A

B. Alternative B

This section should identify options and alternatives to the proposed SMP project, and the strategy used to identify and define them. Include a description of the approaches for identifying alternative ways to plan for security management such as:

- Reuse of existing system components versus building new or buying
- Outsource versus in-house development of systems
- Commercial off-the-shelf versus proprietary

For each alternative, include cost/benefit analysis, initial and ongoing costs, payback period, ROI, and alternative funding sources.

V. Preferred Solution

A. Financial Considerations

Provide a list of identified funding sources for all project components, include the development of the SMP. Include items such as CIP costs, operating costs, total cost of ownership, impact on other projects, and funding requirements.

B. Preliminary Strategy for Acquisition

If known, provide preliminary strategic direction for acquisition. This may include existing procurement contracts, existing vendor relationships, and a description of the communications needed for acquisition requirements.

C. Preliminary Work Breakdown Structure

Provide a preliminary Work Breakdown Structure that defines the scope of project work to be accomplished and displays graphically such as Table 12 Project Charter example below:

D. Assumptions and Constraints

Provide a detailed explanation of assumptions and constraints that may accompany the development of the SMP, and stakeholder and vendor relationships.

PROJECT CHARTER EXAMPLE

A Project Charter is defined as a document that provides the main purpose or intended goal, identifies stakeholders, and delineates roles and responsibilities, including the lead project manager as the reference of authority. The charter is used by the airport as the guideline for starting the SMP process. Planners can populate the template in Table B-2 with the data from the Business Case once it has been reviewed and approved by airport management. This Project Charter becomes the governing document used to implement the SMP process.

Table B-2. Project Charter Example

Project Charter	
(1) Project Title	
(2) Project Scope Abstract	

(3) Project Manager	(3) Level of Authority	(4) Project Sponsor(s)	(5) Type of Project Sponsor

(6) Product Description / Deliverables	
(7) Project Objectives	
(8) Work Site	
(9) Pre-assigned Resources	

(10) Stakeholders List		
Name	Title	Organization

(11) Summary Milestone Schedule	
Description	Due Date

(12) Summary Budget	
(13) Assumptions	(13) Constraints
(14) High Level Project Risks	

Part II – Business Information	
(15) Main Contract Terms & Conditions	
(16) Business Case	
(17) Stakeholders Main Expectations	
(18) Stakeholders Engagement	
(19) Stakeholders Requirements	
(20) Success Criteria	

Part III – Organizational Information	
(21) High Level Process Improvement Plan	
(22) Organizational Process Definition	
(23) Main Lessons Learned Applied	
(24) Tools & Templates	

Signature(s)/Dates

Project Sponsor(s)

Project Manager

Disclaimer: This document has been developed based on a template provided by projectmanagement.com and material from the template has been reproduced with permission from Project Management Institute, Inc.

APPENDIX C: PROJECT MANAGEMENT PLAN (EXAMPLE)

The Project Management Plan is the document used to capture the Business Case, Project Charter, and Stakeholder list, as well as other management plans (e.g., communication plan, travel plan, etc.)

I. Scope

   a. Project Information

   b. Project Description and Background

II. Terms and Acronyms

III. Applicable Documents

IV. Project Overview

   a. Project Business Case

   b. Project Charter

V. Assumptions and Risks

VI. Organizational Responsibilities and Authority

VII. Tasks Definition and Work Breakdown Structure

VIII. High-Level Long-Range Strategy and Analysis

   a. Benchmarking

   b. Market Research

   c. Staffing Assessment

   d. Airport Trend Research and Future-Proofing

   e. Financing

   f. Labor Demand Forecast

   g. Compensation Study

   h. Retention Analysis

IX. Budget

   a. Road Mapping

X. Reporting and Communication

   a. Points of Contact

   b. Meetings

XI. Project Tracking and Controls

XII. Management Plans

a. Scope Management Plan

b. Schedule Management Plan

c. Cost Management Plan

d. Quality Management Plan

e. Communication Management Plan

f. SSI Control Plan

g. Risk Management Plan

h. Procurement Management Plan

i. Change Management Plan

APPENDIX D: MODEL SSI CONTROL PLAN

Developing an SMP will require the SMPT to obtain as well as develop SSI in accordance with TSR 49 CFR § 1520. At a minimum, the following information must be included. It is recommended that this information be reviewed with the airport's ASC prior to the start of the SMP.

Access to SSI

Access to SSI is based on need to know. An airport employee has a need to know SSI when access to the information is necessary for the employee to conduct official duties. A contractor employee has a need to know SSI when access to the information is necessary for that employee to carry out a requirement of a contract relating to transportation security.

Marking SSI

Any person who creates a document containing SSI must include a protective marking and limited distribution statement that clearly identifies the information as SSI, and specifies the distribution limitation required. A person who receives a record containing SSI that is not marked accordingly must add such marking and inform the sender of its omission.

The protective marking, **SENSITIVE SECURITY INFORMATION**, must be written or stamped in plain-style bold type, such as Times New Roman font size 16, or an equivalent style and font size. For documents, it must be applied at the top of the outside of any front cover (including a binder or folder), on the top of any title page, on the top of the first page and each subsequent page, and on the top of the outside of any back cover (including a binder or folder). This marking should be placed in a comparable location on charts, maps, or drawings and on film, video, or electronic media. A typical SSI protective cover sheet is shown in Figure D-1.

A distribution limitation statement must be applied at the bottom of the outside cover of any front cover (including a binder or folder), on the bottom of any title page, on the bottom of the first page and each subsequent page, and on the bottom of the outside of any back cover (including a binder or folder). It should be placed in a comparable location on other forms of media. The distribution limitation statement should be written or stamped in plain-style bold type, such as Times New Roman font size 8, or an equivalent style and font size. This statement must read as follows:

"WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR 1520. No part of this document may be released to persons without a need to know, as defined in 49 CFR 1520, except with the written permission of the TSA Administrator, Washington, DC. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public release is governed by 5 U.S.C. 522."

Documents that transmit SSI but do not themselves contain SSI must be marked with the distribution limitation statement. In addition, the following statement must be affixed to the front page of the transmittal document.

"The protective marking SENSITIVE SECURITY INFORMATION and/or the distribution limitation statement on this document are canceled when the attachments containing SSI are removed."

Safeguarding SSI

All personnel possessing SSI are responsible for ensuring that such information is always safeguarded from disclosure to unauthorized persons. When the information is not under the individual’s direct physical control, the individual is responsible for ensuring that it is safeguarded and protected so that it is not physically or visually accessible to persons who do not have a need to know. When unattended, SSI must be secured in a locked container, office, or other restricted access area, with access to the keys or combination limited to those with a need to know.

Packaging and Transmitting SSI

SSI may be transmitted by US Postal Service first class mail or regular parcel post, or by other delivery services such as FedEx or UPS. It must be double wrapped and enclosed in an opaque outer envelope or other opaque wrapping. Addressing the package with an attention line containing the name and office of the recipient helps to ensure that the SSI material is received and opened only by authorized personnel. The inner envelope must be addressed to the recipient with a statement that the material contained within is SSI and must be opened only be the authorized addressee.

When hand-carried within or between buildings, SSI must be protected by a cover sheet, protective folder, distribution pouch, or other method to prevent visual disclosure.

When transmitted by email, SSI must be in a password-protected attachment. The passwords and procedures must comply with standards set by the airport’s ASC. When no specific procedure is provided, the SMPT will, at a minimum, create a password. Passwords cannot accompany the protected file.

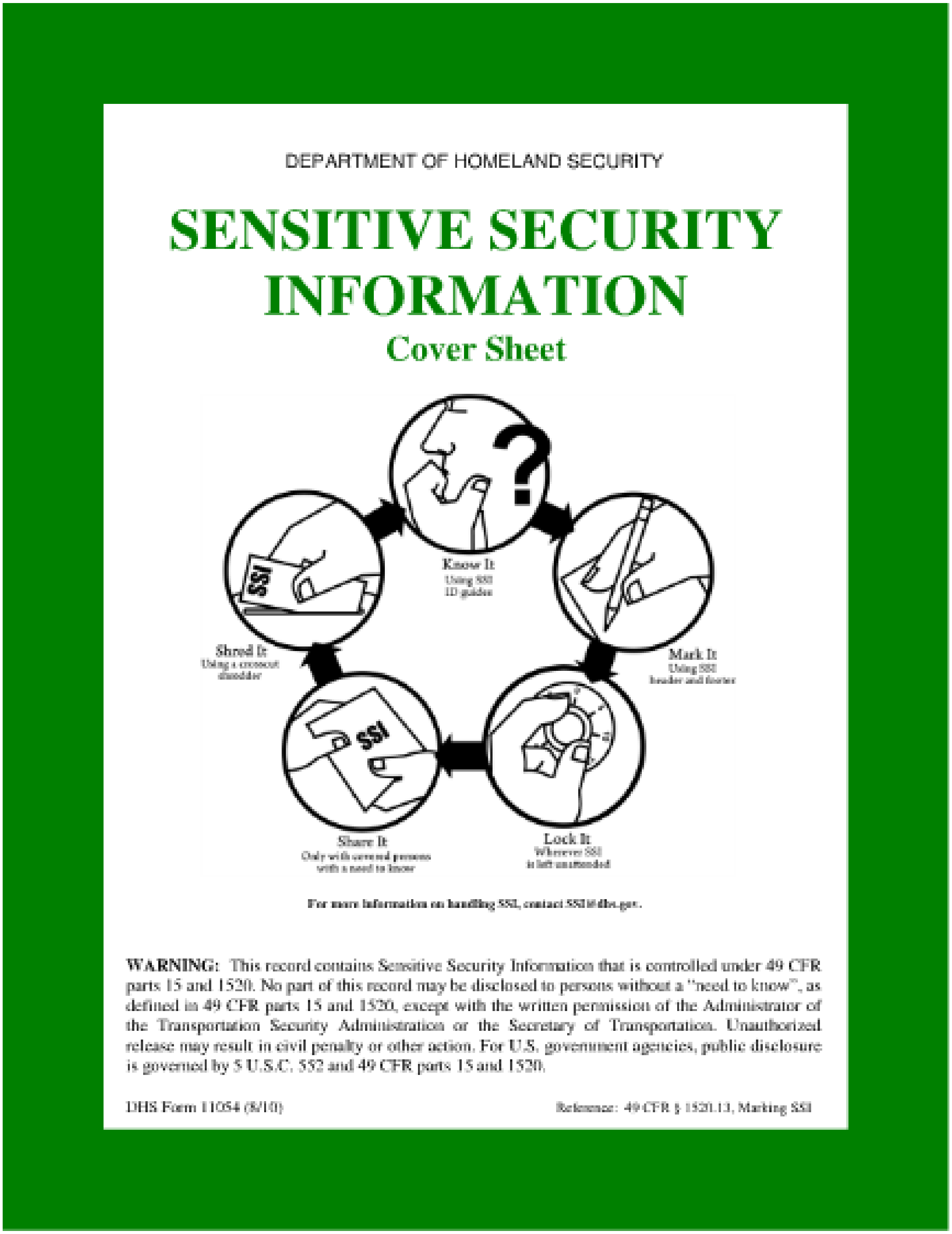
When sending SSI by fax, the sender must ensure that the receiving fax machine is in a secure area or that an authorized recipient is at the receiving fax machine to promptly retrieve the information.

When communicating SSI by telephone, the caller must ensure that the person receiving the SSI is an authorized recipient. Cellular and cordless telephones should be avoided if possible, because such conversations are easier to intercept and monitor.

Destruction of SSI

SSI should be destroyed in a manner that ensures that recovery of the sensitive information would be difficult, if not impossible. Any means approved for the destruction of national security classified material may also be used for SSI. When no airport-specific policy or procedure exists, the SMPT’s preferred method is shredding.

Figure D-1. Typical SSI Cover Sheet



DEPARTMENT OF HOMELAND SECURITY

SENSITIVE SECURITY INFORMATION

Cover Sheet

Know It
Using SSI ID guides
Mark It
Using SSI header and footer
Lock It
Wherever SSI is left unattended
Share It
Only with covered persons with a need to know
Shred It
Using a crosscut shredder
SSI
SSI

For more information on handling SSI, contact SSI@dhs.gov.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

DHS Form 11054 (8/10) Reference: 49 CFR § 1520.13, Marking SSI

APPENDIX E: EXAMPLES OF SMP DOCUMENTATION FRAMEWORK

Table E-1. Example of Existing Conditions Review Framework

EXISTING CONDITIONS SUMMARY				
SYSTEM	**TYPE**	**STATUS/CONDITION**	**ASSESSMENT**	**COMMENTS**
PHYSICAL ACCESS CONTROL				
Physical Access Control System (PACS)	Lenel Picture Perfect (1800 C/R)	End of Life	B	Needs to be replaced, End of Life/Insufficient Reporting Capability/Proprietary closed hardware
Remote Gate Control	Genie - Linear Model 11 (8/10 Gates)	Unsupported	B	Needs to be replaced/No Monitoring/No CCTV
CBP Man Trap System	Programmable Logic Controller Based Interface	Unknown	B	Airport are moving away from PLX based systems
Biometric Verification System	Ingersoll Rand Hand Key Light	Nearing End of Life	M	Should be replaced
High Security Brass Key	Intellikey	End of Life	M	Needs to be replaced/Needs to be integrated with IDMS
ID BADGING				
Access Control Office	Process	Poor/Paper Driven	B	Process is not optimized
ACMS/Credentialing	QS - SAFE	Current * In Progress	E	In early stages of implementation
	B - Below Industry Standards			
	M - Meets Industry Standards			
	E - Exceeds Industry Standards			

Table E-2. Example of Gap Analysis Study Framework

Item #	Task 104 - Security Master Plan Needs Assessment Findings	Relative Priority	Business Process	Organization	Technology	Physical	Comments
1.0	**Airport Security Related**						
1.1	Develop a Perimeter Surveillance Capability	M	Take into consideration Airport Master Plan and the need to optimize the number of portal gates. Establish a standard for any future portal gates or building on the perimeter to include surveillance.	Ownership of perimeter surveillance capabilities needs to be decided between operations and security. Funding needs to be committed to design and implementation capability.	Presently the CCTV system cannot fully observe the perimeter. The types of cameras and video management system would need to be designed.	Currently limited power and communications infrastructure, mostly around existing buildings and gates. This would need to be supplemented.	

Table E-3. Example of Recommendation Summary Table

Recommendations Summary Table			
Section	**Recommendation**	**Summary of Recommended Project**	**Priority**
9.3	Command & Control Systems Technology	Implement a PSIM/Common Operating Environment and consider use in a consolidated facility	Medium
9.4	Physical Access Control System Replacement	Replace the currect PACS, create an airport standard for access controlled doors, vehicle gates, and programmable smart key systems	High
9.5	Video Surveillance System Upgrade	Upgrade the current Video Surveillance and Video Management System installations, create an airport standard for CCTV Camera use and placement	Medium
9.6	Standard Security Boundary Design and Specifications	Create airport standards for security fencing and barrier and bollard configurations with acceptance criteria	Medium
9.7	Barrier and Fence Upgrades	Review and remediate AOA perimeter fencing and establish clear zones	Medium
9.8	Storm Drain Security	Perform a detailed review and assessment of all storm drain and outfall structures and implement access control and alarm monitoring functionality in order to secure these structures	High
9.9	Perimeter Intrusion Detection System Development	Perform a detailed Perimeter Exisiting Conditions Assessment and then a detailed design for PIDS implementation	Medium
9.10	Gate Automation and Enhanced Gate Technology	Evaluate and develop the requirements for implementation of Gate Automation and Enhanced Gate access control technology for all AOA gates	Medium

Table E-4. Example of Recommendation Framework

Item #	Security Master Plan	Relative Priority	Business Process	Organization	Technology	Physical	Comments
1.0	**Infrastructure**						
1.1	Inner and Outer Loop	H	Admin functions now share the same physical core network as safety and security systems	Experienced network engineer needed to support system	New switches and core equipment for redundancy	New core rooms and expanded TRs	Ongoing design in SIMP project
2.0	**Access Control**						
2.1	Conversion to new access control panels and card readers w/ dual technology for a year, then all smart card technology after conversion	H	Badging Office will use different type of reader	Service from contractors to remain in effect for new system	Current ACS Technology is nearing the end of its life, upkeep and maintenance costs will continue to increase, possible system failure or breach of security continues to increase	Current TR may not be large enough to accommodate racks for IP-based ACS	Smart cards more expensive, but more secure

Item #	Security Master Plan	Relative Priority	Business Process	Organization	Technology	Physical	Comments
2.2	Biometric Reader installation for increased security	L	Change in badging procedure and management of data	N/A	Network will require lower latency and increased port counts for biometric readers	Current TR may not be large enough to accommodate racks for IP-based biometrics	Readers more expensive, technology not fully developed or reliable
3.0	**CCTV**						
3.1	Analog to IP Conversion	M	New process needed for renovations to terminal and other areas, dictating when to replace camera with IP, use original analog, or place additional coverage	Position responsible for verifying camera location, placement, and connectivity	IP conversion will require more ports on nearby switches	Current TR may not be large enough to accommodate racks for IP-based camera	All cameras should be routinely replaced every 5–7 years. Cycle would need to be established.
3.2	New Camera Coverage	M	Coverage request process needed for tenants in the facility who wish to use the system or add additional coverage	Increase in camera counts increases support requirements, need oversight committee for new camera additions	Increased port counts and integration of new cameras	Current TR may not be large enough to accommodate racks for IP based cameras	
4.0	**Perimeter Detection**						
4.1	Perimeter Risk Assessment	M	Hire an outside consultant to perform independent risk assessment on the perimeter and cargo areas	No new staff, project manager assigned to risk-assessment project	Assessment will not require new technology; future recommendations are contingent upon results	N/A	Possible joint vulnerability assessment may fulfill this requirement
4.2	Culvert Coverage and Detection	H	Implement process to maintain and validate culvert coverage and detection	No new staff, assign part 139 inspection crew to add this to their checklist	Possible laser or other detection capability, along with connectivity to main network	Power needed for culvert monitoring	
5.0	**Fire Alarm Monitoring**						
5.1	All new buildings and tenants installed with point identifiable system	M	Begin process and change lease agreements so that new tenants and those who are upgrading/renovating their areas must install point identifiable alarm panels	Tenants provide service and upkeep of their own panels	Possible integration in future PSIM for alarm correlation.	Changes to tenant spaces	This is a direct request from the local fire marshal
6.0	**Physical Security Information Management (PSIM)**						
6.1	Implement a PSIM for use by management and in the Emergency Operations Center	L	Complete operational change for multiple departments. Study must first be conducted before purchase of software.	Staff required to implement, integrate, and upkeep of the PSIM	Purchase of software, very little hardware changes	N/A	

Item #	Security Master Plan	Relative Priority	Business Process	Organization	Technology	Physical	Comments
7.0	**Test Environment**						
7.1	Offline version/limited capability of all security systems deployed; for use in testing devices before large-scale field deployment	M	Additional step when purchasing new hardware or software	No full-time staff required, room will be utilized by multiple stakeholders	Requires an isolated, separate network with ISP connection for remote vendor access	500–1000 sq. ft. of test lab space	
8.0	**Exit Lane Technology**						
8.1	Unmanned Exit Lane infrastructure	M	N/A	Reduction in staff needed to monitor exit lanes	Possible infrastructure and monitoring needs, depending on assessment of space needing coverage	Major modifications to security checkpoint space	

APPENDIX F: AIRPORT RISK AND VULNERABILITY ASSESSMENT RESOURCES

I. Introduction and Background

Security is a process of risk management, identifying threats, and assessing how vulnerable the airport might be to various types of threats and scenarios, including their consequential actions.

Threats and vulnerabilities cover a wide array of events, virtually none of which can be eliminated while the airport system is in operation. Since no system can be rendered totally secure, once threats and vulnerabilities are identified, their impact on the total system must be assessed to determine whether to accept the risk, and the extent to which corrective measures can reduce their severity.

Threats are specific activities that are likely to damage the airport's facilities, personnel, and/or patrons. Threats range from the extreme of terrorist-initiated bombs or hostage-taking to more common events such as theft of services, pick-pocketing, graffiti, and vandalism. Those responsible for identifying and assessing threats and vulnerabilities must not only measure the degree of potential danger but also determine the chances of that danger occurring, define what preparations and actions are needed to mitigate such events, and then consider and prioritize what resources are available for response and recovery. Airports also must consider the possibility of multiple simultaneous events that may or may not be related.

Vulnerability is the susceptibility of the airport and its systems to a security hazard. Vulnerabilities are commonly prioritized through the creation of scenarios that pair identified assets and threats. A risk analysis must be undertaken to determine which vulnerabilities take the highest priority. This is best done during the initial ConOps process, when operational requirements are established, and should be extended into the design and construction of a facility and its technological systems, since an increased priority in one area typically means another area will receive less attention. Also wielding considerable influence in the design decisions is the way a facility is operated (e.g., security procedures and practices or administrative and management controls, including staffing considerations).

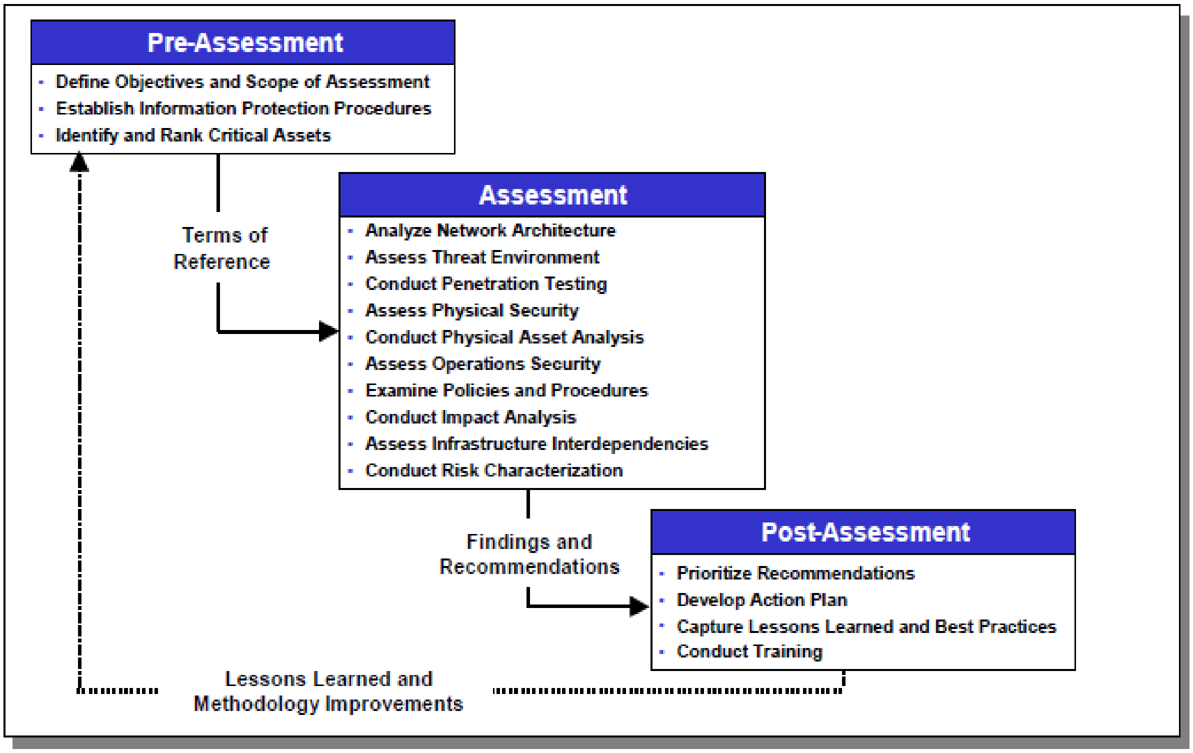
An airport vulnerability assessment is a tool for determining the extent to which an airport facility may require security enhancements. It serves to bring security considerations into the mix early in the design process rather than as a more expensive retrofit.

II. The Assessment Process

Threat and vulnerability assessments provide an analytical process for considering the likelihood that a specific threat will endanger the targeted facilities and their systems (see Figure F-1). Using the results of a capabilities assessment, threat and vulnerability analyses can also identify activities to be performed to (a) reduce the risk of an attack and (b) mitigate the consequences of an attack.

Assessments typically use a combination of quantitative and qualitative techniques to identify security requirements, including the historical analyses of past events, intelligence assessments, physical surveys, and expert evaluation. When the risk of hostile acts is greater, these analytic methods may draw more heavily upon information from intelligence and law enforcement agencies regarding the capabilities and intentions of the aggressors.

Figure F-1. Vulnerability Assessment Phases


Pre-Assessment
Define Objectives and Scope of Assessment
Establish Information Protection Procedures
Identify and Rank Critical Assets
Terms of Reference
Assessment
Analyze Network Architecture
Assess Threat Environment
Conduct Penetration Testing
Assess Physical Security
Conduct Physical Asset Analysis
Assess Operations Security
Examine Policies and Procedures
Conduct Impact Analysis
Assess Infrastructure Interdependencies
Conduct Risk Characterization
Findings and Recommendations
Post-Assessment
Prioritize Recommendations
Develop Action Plan
Capture Lessons Learned and Best Practices
Conduct Training
Lessons Learned and Methodology Improvements

Source: US Department of Energy

Several risk management tools can be used to assess risk and vulnerability at an airport, including those in standards and commercially available products. An unstructured and fragmented assessment plan only makes framing risk management more difficult. Providing a consolidated and comprehensive security risk management program as a guide to the industry can help avoid these issues. The tools listed herein are provided for the SMPT as an aid in evaluating and establishing the assessment process.

An important airport resource is the National Safe Skies Alliance PARAS 0004 *Recommended Security Guidelines for Airport Planning, Design, and Construction.* Appendix A contains summaries of several resources. A complete bibliography of the materials reviewed is contained in the references section of this report. These guidelines are not government regulations and requirements, but a compendium of real-world experiences and best practices, providing recommendations for airport-security-specific planning and design concepts that are scalable to airports of any size and complexity.

III. Risk and Vulnerability Assessment Methodology Resources

1. Pugh Matrix

The Pugh matrix helps determine which items or potential solutions are more important than others.

It is a scoring matrix used for concept selection in which options are assigned scores relative to criteria. The selection is made based on the consolidated scores. Before starting a detailed design, there are many options—this tool, also known as a criteria-based matrix, helps with selecting the best option.

The Pugh matrix is a tool used to facilitate a disciplined, team-based process for concept generation and selection. Several concepts are evaluated according to their strengths and weaknesses against a reference concept called the datum (base concept). The datum is the best current concept at each iteration of the matrix.

The Pugh matrix allows an individual or team to:

1. Compare different concepts
2. Create strong alternative concepts from weaker concepts
3. Arrive at an optimal concept that may be a hybrid or variant of the best of other concepts

This matrix encourages comparison of several different concepts against a base concept, creating stronger concepts and eliminating weaker ones until an optimal concept finally is reached. It does not require a great amount of quantitative data on design concepts, which generally is not available at this point in the process.

(iSixSigma, https://www.isixsigma.com/dictionary/pugh-matrix/)

2. Information Security Risk Assessment Frameworks

   a. NIST Guide for Conducting Risk Assessments

This resource provides relevant information for security program fundamentals when dealing with enterprise risk assessments and IT security. A comprehensive risk assessment approach that leads to effective mitigation planning is described in detail. Specific guidance is given to key risk assessment concepts, such as compliance with government regulations, standards, frameworks and guidelines, and differences in IT and physical security TVAs.

Resource Link: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

- Who is this resource intended for?
  - This resource is intended to serve a diverse group of risk management professionals including:
    - Individuals with oversight responsibilities for risk management (e.g., heads of agencies, CEOs, chief operating officers, and risk executives)
    - Individuals with responsibilities for conducting organizational missions/business functions (e.g., mission/business owners, information owners/stewards, and authorizing officials)
    - Individuals with responsibilities for acquiring IT products, services, or information systems (e.g., acquisition officials, procurement officers, and contracting officers)
    - Individuals with information system/security design, development, and implementation responsibilities (e.g., program managers, enterprise architects, information security architects, information system/security engineers, and information systems integrators)
- How would airports consider implementing this resource?
  - Airports interested in analyzing day-to-day IT infrastructure security operations and who are expecting large growth in passenger traffic would find this resource useful. This document lays out the organizational structure of airport technical systems in a

way that airports can identify potential threats, monitor system performance, and implement training for a sustainable cybersecurity program.

- Is the document regulatory, guidance, information only, or all of these?
  - The document is primarily guidance- and information-based. Cases from selected commercial airports can be used as guidance and general best practices in technology-based approaches to airport vulnerability planning. The guidebook provides airport managers with resources to mitigate inherent risks of cyberattacks on technology-based systems.

b. NIST Performance Measurement Guide for Information Security

This resource supports airport operators in their development and selection of security measures to be used at the information system and program levels. Detailed guidance on the effectiveness of information system and program security controls for an agency to achieve its mission is provided to the user. The resource also helps the user categorize IT infrastructure threats and employ a technology-based approach to airport security and implement countermeasures in airport systems.

Resource Link: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

- Who is this resource intended for?
  - For airports interested in measuring security control effectiveness and analyzing day-to-day information security operations. This resource is primarily created for airport operators who are familiar with security controls, specifically:
    - Chief Information Officers
    - Senior Agency Information Security Officers
    - System Security Officers
- Is the document regulatory, guidance, information only, or all of these?
  - The document is primarily guidance-based. Cases from selected commercial airports can be used as guidance and general best practices in technology- and cyber-based approaches to airport vulnerability planning. The guidebook provides airport managers with regulatory and strategic information to mitigate inherent risks of cyberattacks on enterprise-based systems.

3. TSA Joint Vulnerability Assessments and Protective Measures Matrix

Airport security departments can begin a vulnerability review exercise by performing a self-administered risk assessment using a TSA-provided template. This activity will survey existing conditions and identify vulnerabilities throughout the airport. Using the Project Management Plan as a baseline document, existing knowledge of facilities, stakeholders, and internal processes will benefit operators as they scan for vulnerabilities in areas such as the airport’s own IT network and communications systems, baggage systems, ACSs, parking management systems, VSS/CCTV, PIDS, eEnabled aircraft systems, document management systems, and radar systems.

The checklist template in Table F-2 is intended to help the airport security department or organization prepare their internal threat assessment with a consistent evaluation of designs at various levels. The checklist can be used as a screening tool for the design of an early-stage vulnerability assessment. Program and design improvement recommendations are available for any category that the airport deems as underprepared.

Resource Link: https://www.tsa.gov/sites/default/files/2017_ga_security_guidelines.pdf

- How airports might consider implementing this resource?
  - The Airport Security Assessment and Protective Measures Matrix is an assessment tool that can help develop a baseline on the status of security measures and the priorities on which the airport may wish to focus. The matrix allows operators to subjectively score their airport in the focus areas from three stages:
    - Pre-event preparedness
    - Detection and response during an event
    - Post-event recovery.

Table F-1 contains the matrix and the specific focus areas that can be observed in an assessment.

- Is the document regulatory, guidance, information only, or all of these?
  - The document is primarily guidance, with step-by-step instructions for determining technology- and non-technology-based vulnerability ratings.

Table F-1. TSA Airport Security Assessment and Protective Measures Matrix

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	PREPAREDNESS	DETECT	RESPOND	RECOVER	COMMENTS
1. AIRPORT SECURITY PLAN					
a. Record of revisions					
b. Table of Contents					
c. Emergency Phone Numbers					
d. Disclosure Statement and Responsibilities					
e. General Information (for example, Foreword, Introduction and Purpose, Distribution, Name & Location, Airport Activities, Airport Description					
f. Definitions & Terms					
g. Administration					
h. Aircraft Movement Areas					
i. Airport Security Procedures					
j. Airport Emergency Grid Map					
k. Identification of Airport Personnel (Incl. TSA GA inspections)					
l. Identification of Vehicles					
m. Law Enforcement & ARFF					
n. Special Event (Incl. National Security Events)					
o. Increased Security Threats					
p. Airport Watch Program					
q. Reward & Feedback Program					
r. Aviation Security Contingency Plans (Incl. Lockdown Procedures, Crisis Counseling)					
s. Airport Continuity of Operations Plan					

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	PREPAREDNESS	DETECT	RESPOND	RECOVER	COMMENTS
t. Exhibits (for example, Airport Emergency Grid Map, Airport Tenant Map, Airport Layout Plan, Bomb Threat Card, Government & Industry Actions, Bomb Blast Stand-off Card, FBO report card, GA Alert Check List)					
u. Other					
2. AIRPORT EMERGENCY PLAN					
a. Record of Revisions					
b. Table of Contents					
c. Emergency Phone Numbers					
d. Definitions & Terms					
e. Preface					
f. Participating Agencies					
g. Assignment of Duties & Responsibilities					
h. Emergency Communications					
i. Crowd Control					
j. Medical Services					
k. Family & Victim Assistance					
l. Public Information					
m. Types of Emergencies & Response Procedures (Alert I, Alert II, Alert III, Structural Fires/Incidents, Severe Storms, Bomb Threats, Sabotage, Hijacking, Power Failures)					

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	PREPAREDNESS	DETECT	RESPOND	RECOVER	COMMENTS
n. Exhibits (Emergency Grid Map, Tenant Address Map, Aircraft Operating Areas, Emergency Staging Areas, Fuel Farm Map, Evacuation Plan, Lockdown Plan, Call Down List, Bomb Threat Card, Suspicious Package Recognition & Handling Plan, ATCT “Zero” Procedure, HazMat Contractor List)					
o. Business Continuity Plan					
p. Other					
3. ACCESS CONTROLS					
a. Controlled entrances (for example, doors, entryways, gates, turnstiles, door alarms)					
b. Control of Materials (for example, , fuel, other)					
c. Secure perimeter (for example, fences, bollards)					
d. Restricted access areas (for example, key assets, roofs, HVAC, fuel farms, electrical vaults)					
e. Access identification (for example, employee badges, biometrics, etc.)					
f. Signage					
g. CCTV					
h. Other					

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	**PREPAREDNESS**	**DETECT**	**RESPOND**	**RECOVER**	**COMMENTS**
4. BARRIERS					
a. Walls, earth banks & berms (blast protection)					
b. Fences (for example, barbed wire, chain link)					
c. Screens & shields (for example, visual screening)					
d. Vehicle barriers (for example, bollards, jersey barriers, planters, vehicles used as temporary barriers)					
e. Other					
5. MONITORING & SURVEILLANCE					
a. CCTV (for example, fixed, pan, IR, Thermal)					
b. Motion Detectors					
c. Fire & Carbon Monoxide Detectors					
d. Explosive Detectors					
e. Chemical Agent Detectors					
f. Biological Agent Detectors					
g. Radiological Agent Detectors					
h. Metal Detectors					
i. Night-vision Optics (IR, thermal)					
j. Lighting (for example, buildings, perimeter)					
k. Other					

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	PREPAREDNESS	DETECT	RESPOND	RECOVER	COMMENTS
6. COMMUNICATIONS					
a. Telephone (for example, land line, mobile, satellite)					
b. Radios (for example, 800 MHZ, VHF, UHF, battery/hand-powered)					
c. Interoperable Equipment (W/ other agencies)					
d. Redundant & Backup Communications Capabilities					
e. Data Lines (for example, internet, perimeter, permanent, temporary, solar/wind powered)					
f. Other					
7. INSPECTION					
a. Check Points (strategic locations, guard shack, etc.					
b. Personnel Searches (for example, employees, visitors, contractors, vendors)					
c. Vehicle searches (for example, cars, trucks)					
d. Aircraft searches (based & transient)					
e. Hangar searches (private, FBO, SASO)					
f. Building searches (all)					
g. Cargo & Shipment searches					

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	PREPAREDNESS	DETECT	RESPOND	RECOVER	COMMENTS
h. X-ray Screening (or known shipper)					
i. Other					
8. SECURITY FORCE(S)					
a. Force Size & Jurisdiction					
b. Equipment (weapons, communications, vehicles, SWAT, specialized incident response gear [CBRNE], etc.)					
c. Training					
d. SOP & Special Operating Procedures (patrols, checkpoints, LE including Local, State and Federal, incl. IGA & LOA, mutual aid agreements)					
e. Coordination among security/response teams (NIMS Training)					
f. Other					
9. CYBER SECURITY					
a. Firewalls (VPN, etc.)					
b. Virus Protection					
c. Password Procedures					
d. Information Encryption					
e. Computer Access Control					
f. Intrusion Detection					
g. Redundant & Back Up Systems					
h. Hosted Sites					

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	PREPAREDNESS	DETECT	RESPOND	RECOVER	COMMENTS
i. Third Party Assessment					
j. Other					
10. SECURITY PROGRAM					
a. Employee Background Checks					
b. Tenant Background Checks					
c. Alternative Background Vetting (RBS)					
d. Visitor Control & Monitoring					
e. Foreign Visitor Security Protocol (for example, FBI)					
f. Security Reporting System					
g. Operations Security Plan (See #2)					
h. Coordination among FBOs, SASOs, tenants & Local, State and Federal Law Enforcement					
i. Other					
11. INCIDENT RESPONSE					
a. Emergency Response Plan					
b. Emergency Response Equipment					
c. Emergency Response Personnel					
d. Emergency Response Training, drills & TTXs					
e. Shelter Facilities					
f. Evacuation Procedures					
g. Communications Internal/External					
h. NIMS					

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	PREPAREDNESS	DETECT	RESPOND	RECOVER	COMMENTS
i. Other					

4. ASIS Security Risk Management Assessment

   This report contains relevant information to security program fundamentals in the utilities sector dealing with working through risk assessments, liabilities, compliance, and IT security.

   The eight sections of this report provide a comprehensive view of security risk for utilities. Initially, risk is defined through the equation Risk = Threat (times) Vulnerability. A comprehensive risk assessment leads to effective mitigation planning, which needs to be conducted in layers. The layers include the following:

   - Liability issues that arise out of inadequate or outdated risk assessments
   - The potential for business losses, societal impacts, environmental damage, and loss of reputation
   - Compliance with government regulations, standards, frameworks, and guidelines
   - Differences in IT and physical security TVAs

   Resource Link: https://www.acq.osd.mil/log/PS/.psc.html/7_Management_System_for_Quality.pdf

5. National Critical Infrastructure Protection Plan Risk Assessment Framework

   This resource contains information relevant to the development of vulnerability planning procedures and covers specific elements of risk such as threat, vulnerability, and consequence for various airport stakeholders.

   Resource Link: https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf

Risk Assessment Tools

- Self-Vulnerability Assessment Tool (SSI) – 2010
- Commercial Airport Resource Allocation Tool (SSI) – 2010
- Airport Security Self-Evaluation Tool Users’ Guide (SSI) – 2011
- Compliance Security Enhancement Through Testing
- Technology-based Assessment Tool for PIDS

TSA Outcome Focus Compliance – 2017

APPENDIX G: FUNDING SOURCES BY STATE

Table G-1 lists samples of different funding sources and mechanisms by state. This list is not intended to be a comprehensive list of every state and region. The samples include:

- State Matching Funds
- Specifications and Quote Documents
- General Fund Appropriations
- X-Year Airport Development Programming (DOT)
- State Aviation Funds
- Aeronautical Funding Programs/AIP Matching Grants
- Discretionary Fund Grant Programs
- State-based Airport Improvement Funds/Grants
- State/Local Bond Fund Types

Table G-1. Security Master Planning: Funding Sources

ALABAMA	
Agency	ALDoT – Aeronatics Bureau
Program/Grant	State Matching Funds
Purpose	Sponsors match grants to support state-funded improvement projects, mainly to enhance operations, public safety, and capacity
Funding	The FAA will fund 90% of an eligible airport improvement project and the local airport owner is responsible for the remaining 10% match. The local airport can request a state matching grant for one-half of its matching obligation, or 5% of the total project
Eligibility	Publicly owned, public use airports for planning and capital improvements to airfield facilities
Source	http://www.dot.state.al.us/ltweb/pdf/ArchivedAnnualReports/2015AnnualReport.pdf https://www.infrastructurereportcard.org/wp-content/uploads/2016/10/ASCE-AL-Report-Card-2015-Full-Report-FINAL-web.pdf
ALASKA	
Agency	Alaska DOT and Public Facilities – Alaska Aviation System Plan
Program/Grant	General Fund Appropriations – Deferred Maintenance and Life Safety Projects (Capital Projects)
Purpose	Documents the existing aviation network, identifies needed airport improvements, sets funding priorities, and proposes aviation policy
Funding	
Eligibility	
Source	http://www.alaskaasp.com/admin/Docs/Rural%20Airport%20Deferred_Maintenance%20Fact%20Sheet.pdf

ARIZONA

Agency	AZDoT
Program/Grant	Five-Year Airport Development Programming
Purpose	Airport Development Grants: State/Local Matching
Funding	To maximize the availability of federal assistance to local airports, it is the State Transportation Board's policy to provide state assistance by funding one-half of the sponsor's local share of FAA AIP grants in AZ.
Eligibility	Projects that are associated with safety of operations, security, capacity, environmental services, and planning, including AMPs, airport site selection, ALP updates, and airport-wide drainage studies.
Source	https://azdot.gov/docs/default-source/airport-development/airport_development_guidelines_oct_2011.pdf

Agency	AZDoT
Program/Grant	State Aviation Fund
Purpose	Made up of monies collected from a variety of sources to be distributed to airports for airport development
Funding	Allocations: Commercial Service Airports (43%); Reliever Airports (35%); GA-Community Airports (19%); GA-Rural (2%); GA-Basic (0.27%)
Eligibility	The airports listed above are eligible. Program initiatives, system needs, or the balance of the fund may require occasional administrative adjustments.
Source	https://azdot.gov/docs/default-source/airport-development/airport_development_guidelines_oct_2011.pdf

CALIFORNIA

Agency	California Transportation Commission
Program/Grant	Aeronautics Program – AIP Matching Grants
Purpose	Increased state funding for AIP planning and development projects
Funding	The state AIP match rate has been set at 5% of the federal grant. Once an FAA AIP Grant has been executed, the sponsoring agency may apply to the state for an AIP matching grant. Grants are processed in the order received and awarded until all funds are exhausted. Depending upon the number of grant applications received, processing time can range between 2 to 3 weeks.
Eligibility	Before applying for an AIP Matching Grant, the project must be included in the most recently adopted CIP. Projects not included in the current CIP are ineligible for state funding.
Source	http://dot.ca.gov/hq/planning/aeronaut/documents/grants_and_loans/State_AIP_Matching_Grant.htm

Agency	State of California
Program/Grant	California Aid to Airport Program – GA
Purpose	Existing federal law authorizes airport sponsors to submit applications to the Secretary of Transportation for financial assistance for airport improvement projects. Under federal law, upon approval by the Secretary of Transportation, the US government may pay for certain project costs
Funding	Annual Credit grant program - $10K/yr for eligible GA airports

Eligibility	The GA airport meets the permit and funding requirements of California Aid to Airport Program Section 4056 and must be a public entity.
Source	http://wrpinfo.org/media/1293/ca_cathey.pdf https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201320140SB616

COLORADO

Agency	CODOT
Program/Grant	Discretionary Aviation Grant Program
Purpose	Utilizing the remaining 35% of tax revenues to serve the maintenance, capital equipment, and developmental needs of Colorado's 74 public-use airports.
Funding	Senate Bill 49 continuously appropriates fuel tax dollars into the Colorado Aviation Fund.
Eligibility	• Airport Planning • Airport Capital Improvement • Land Acquisition • Aviation Education • Safety and Security
Source	https://www.codot.gov/programs/aeronautics/PDF_Files/WIMSManual_063016 https://www.codot.gov/programs/aeronautics/AviationGrants

CONNECTICUT

Agency	CTDOT
Program/Grant	Transportation Infrastructure Improvement Program
Purpose	Development and improvement of GA airport facilities including grants-in-aid to municipal airports
Funding	Total FY 16 Authorization: $2,000,000
Eligibility	GA Airports
Source	https://www.cga.ct.gov/ofa/Documents/year/SBC/2016SBC-20150728_Analysis%20of%20State%20Bond%20Commission%20Agenda%20Items%20for%20July%2028,%202015%20Meeting.pdf

FLORIDA

Agency	FDoT
Program/Grant	Strategic Airport Investment Projects – Aviation Program
Purpose	Provide funding for strategic infrastructure development opportunities at airports in the state of Florida. Projects are categorized into four primary categories within this program: Critical, Needed, Desired, and Future.
Funding	The department may fund up to 50% of the portion of eligible project costs, which are not funded by the federal government except that the department may initially fund up to 75% of the cost of land acquisition for a new airport or for the expansion of an existing airport that is owned and operated by a municipality, a county, or an authority, and shall be reimbursed to the normal statutory project share when federal funds become available or within 10 years after the date of acquisition, whichever is earlier.
Eligibility	FDOT is authorized to provide up to 100% funding for commercial and GA airport projects that meet the following criteria: provide important access and on-airport capacity improvements; provide capital improvements to strategically position the state

	to maximize opportunities in international trade, logistics, and the aviation industry; achieve goals of an integrated intermodal transportation system; and demonstrate the feasibility and availability of matching funds through federal, local, or private partners.
Source	http://www.flsenate.gov/Laws/Statutes/2011/332.007 http://www.fdot.gov/aviation/pdfs/Strategic%20Guidance%20-%20Airport%207.1.14.pdf
Agency	FDoT
Program/Grant	TRIP
Purpose	Provides funding to regionally significant transportation facilities in regional transportation areas defined by Florida statute
Funding	State funds are available throughout Florida to provide incentives for local governments and the private sector to help pay for critically needed projects that benefit regional travel and commerce. Funds are allocated to districts based on a factor derived from equal parts population and motor fuel collections.
Eligibility	Funding must support facilities that serve national, statewide, or regional functions. The facility must function as an integrated regional system (a transportation project that is associated with a facility that serves regional transportation needs, such as access to and from the area outside of the region, major activity centers in the region, major planned developments such as new retail malls, sports complexes, etc., or transportation terminals).
Source	http://www.fdot.gov/programmanagement/LP/TRIP/TRIPFactsheet.pdf http://www.fdot.gov/programmanagement/LAP/pdfs/Training/D3LATS/2016-2017%20TRIP.PDF

GEORGIA

Agency	GADOT
Program/Grant	Airport Aid Program
Purpose	The Aviation Program has the responsibility of ensuring that publicly owned airports in Georgia are safe, adequate, and well maintained.
Funding	Two primary functions in providing aid: Airport Development and Airport Planning
Eligibility	Airports must enter their 5-Year CIPs and Applications, as well as provide information on fuel sales, based aircraft, wait lists, and consultant information.
Source	http://www.dot.ga.gov/IS/AirportAid

ILLINOIS

Agency	IDOT - Aeronautics
Program/Grant	General Revenue Fund and Series B Bonds
Purpose	Promote and provide safe, cost-effective transportation in ways that enhance the quality of life, improve multi-modal connectivity, foster economic prosperity, and demonstrate respect for the environment.
Funding	General Revenue Fund is derived from all the tax and fee sources that are allocated to that fund. The various public transportation funds are funded through General Revenue Fund transfers. Federal funds are from federal sources.
Eligibility	There are 110 public-use airports in Illinois, of which 77 are publicly owned and eligible for public funding.
Source	http://www.illinoistransportationplan.org/pdfs/transportation_funding_090512_web.pdf

Agency	ILDOT - Aeronautics
Program/Grant	Federal Airport and Airway Trust Fund
Purpose	"Promote and provide safe, cost-effective transportation in ways that enhance the quality of life, improve multi-modal connectivity, foster economic prosperity, and demonstrate respect for the environment."
Funding	Capital funding is primarily provided by the FAA from the Federal Airport and Airway Trust Fund.
Eligibility	There are 110 public use airports in Illinois, of which 77 are publicly owned and eligible for public funding.
Source	http://www.illinoistransportationplan.org/pdfs/transportation_funding_090512_web.pdf

INDIANA

Agency	INDOT – Office of Aviation
Program/Grant	Federal Matching Grants
Purpose	The Indiana Department of Transportation's (INDOT's) Airport Development Fund program is used to develop the 70 Indiana State Aviation System Plan public-use airports that are critical to the Indiana air transportation system.
Funding	The matching rate will depend on available funding at the time the grant is approved.
Eligibility	An Indiana airport, except Indianapolis International Airport, that receives an FAA airport grant is eligible for a state Federal Matching Grant.
Source	http://www.state.in.us/indot/files/Aviation_AirportDevelopmentFundProcedure_090113.pdf
Agency	INDOT – Office of Aviation
Program/Grant	State/Local Grants
Purpose	The Indiana Department of Transportation's (INDOT's) Airport Development Fund program is used to develop the 70 Indiana State Aviation System Plan public-use airports that are critical to the Indiana air transportation system.
Funding	State/Local grant up to a maximum of 50% of projects' eligible costs
Eligibility	The eligible State/Local projects shall include, but are not limited to: • Runway extensions • Terminal buildings (new construction or remodel) • Hangars, including maintenance and overnight transient corporate storage facilities • Aircraft fuel services
Source	http://www.state.in.us/indot/files/Aviation_AirportDevelopmentFundProcedure_090113.pdf

IOWA

Agency	Office of Aviation and Approved by the Iowa Transportation Commission
Program/Grant	GA Vertical Infrastructure Program (GAVI) – State Aviation Program
Purpose	Preservation and development of the vertical infrastructure at GA airports
Funding	Funded through annual appropriations from the state legislature for GA and commercial air service airports

Eligibility	Safety related grant programs (operational emergencies, pavement maintenance, and wildlife mitigation) and airfield development, air service development, land use planning, and vertical infrastructure grants
Source	https://iowadot.gov/aviation/airport-managers-and-sponsors/state-funding/state-funding-programs https://iowadot.gov/aviation/pdfs/4Section2StateAviationGrantPrograms.pdf

MARYLAND

Agency	MDOT
Program/Grant	Consolidated Transportation Program
Purpose	Capital projects that are generally new, expanded, or significantly improve facilities or services that may involve planning, environmental studies, design, right-of-way acquisition, construction, or the purchase of essential equipment related to the facility or service
Funding	Six-year capital budget for transportation projects (FY 2018 –2023)
Eligibility	Planning and Capital Programming Projects
Source	http://www.mdot.maryland.gov/newMDOT/Planning/CTP/Index.html

MASSACHUSETTS

Agency	MassDOT
Program/Grant	Airport Safety and Maintenance Program (ASMP)
Purpose	“Authorized the establishment and administration of a program to assist in the maintenance and repair of airports included in the state airport system plan (SASP), excluding those airports owned and operated by the Massachusetts Port Authority.”
Funding	Appropriated funds are derived from aircraft registration fees, aviation gas tax, and fees for air transportation charged to other state agencies.
Eligibility	To be eligible for a grant, the project must be included in MassDOT’s statewide CIP. Projects are often programmed for routine maintenance, which addresses deficiencies noted in an annual state airport inspection, but airport planning and new construction are also considered eligible projects under the ASMP. ASMP grants are typically issued to airport sponsors for Airport Planning and Airport Development.
Source	http://www.massdot.state.ma.us/aeronautics/FundingPrograms.aspx

MICHIGAN

Agency	MDOT – Aeronautics Commission
Program/Grant	State Aeronautics Fund – Airport Awareness Program
Purpose	The purpose of this category is to increase public awareness of community airports and available air passenger and cargo services, encouraging use of the local airport through education increases awareness of the facility, acceptance of new advanced commuter aircraft, and a better understanding of schedules, destinations, and fares.
Funding	The actual frequency of available funds will vary depending on program appropriation and the number of grants requested, with a goal of 30% of the total program funds to be allocated to this category.
Eligibility	Must complete a grant evaluation with the purpose of the project and description of the airport’s proposed Airport Awareness Activity Plan included

Source	https://www.house.mi.gov/hfa/Archives/PDF/AeronauticsProgramsMemo.pdf https://www.michigan.gov/documents/aero/Air_Service_Program_Guidelines_377697_7.pdf
Agency	MDOT – Aeronautics Commission
Program/Grant	Capital Improvement and Equipment Program
Purpose	The purpose of this category is to improve airport facilities for passenger acceptance, cargo handling, and airport operations to support air service and economic development.
Funding	The actual frequency of available funds will vary depending on program appropriation and the number of grants requested, with a goal of 50% of the total program funds to be allocated to this category.
Eligibility	This program category will allow Michigan airports another funding mechanism for projects currently not undertaken through existing federal and state improvement programs, such as interior terminal modifications, security equipment, flight information centers, defibrillators, ticket areas, ADA accessibility improvements, and cargo handling facilities. The airport must be listed in the Michigan Aviation System Plan.
Source	https://www.michigan.gov/documents/aero/Air_Service_Program_Guidelines_377697_7.pdf

MINNESOTA

Agency	MnDOT – Aeronautics and Aviation
Program/Grant	Airport Construction Grant Program
Purpose	Funds most capital improvements at state system airports based on a determination that the improvement is a justifiable benefit to the air-traveling public
Funding	Maintenance and Operations grants sustain the system utilizing adjustable rates. Maintenance and Operations continues at a higher level with the state share planned to continue at 75%.
Eligibility	Airports in the National Plan of Integrated Airport Systems
Source	http://www.dot.state.mn.us/aero/airportdevelopment/fundingandgrants.html
Agency	MnDOT – Aeronautics Commission
Program/Grant	Airport Maintenance and Operation Program
Purpose	Improvement of airport infrastructure
Funding	The State Airport Maintenance and Operation Grant Program provides two-thirds of state reimbursement to the state system airports for their documented routine maintenance expenses up to a certain ceiling amount that is categorized by airport infrastructure.
Eligibility	The day-to-day labor, material, equipment, and utility expenses of maintaining airport pavements, airport grounds, lighting systems, buildings, and maintenance equipment are eligible costs.
Source	http://www.dot.state.mn.us/aero/airportdevelopment/fundingandgrants.html

NEW YORK

Agency	NYSDOT
Program/Grant	Airport Capital Grant Program (2017)

Purpose	"Funding to preserve and improve airport infrastructure in support of safety, preservation of assets, and economic health of the localities and state."
Funding	NYSDOT solicited applications from eligible applicants between March 28, 2017 and May 2, 2017. Up to $20 million will be awarded for airport capital projects during this fiscal year. No less than $10 million will be awarded to airports located in the upstate region. The state share for any project awarded because of this solicitation shall not exceed $1,500,000.
Eligibility	• The airport must be a public-use airport. • The airport must be listed in the most recent SASP, 2008, which was published in 2009. A list of SASP airports can be found on Table 1 (page 3-4) of the report available at: www.dot.ny.gov/divisions/operating/opdm/aviation/documents. • The airport must have a current Airport Layout Plan (ALP) approved by the FAA and NYSDOT. A copy of the most recent approved ALP will be required prior to contract execution and is encouraged as part of the application submission. • The airport sponsor must be registered in the NYS Grants Gateway System. Not-for-Profit entities must also complete the pre-qualification process in NYS Grants Gateway. For information on the Grants Gateway, visit: www.grantsgateway.ny.gov. • The airport must have a current registration and security plan on file with NYSDOT in accordance with the 2004 GA Airport Security Law (Article 2, Section 14m of Transportation Law). • Sponsors are reminded that they must also meet all FAA requirements related to the airport work to be funded.
Source	https://www.dot.ny.gov/divisions/operating/opdm/aviation/repository/NoticeofFundingAvailability_1.pdf
	NORTH CAROLINA
Agency	NCDOT DoA
Program/Grant	State Airport Aid
Purpose	State Airport Aid is the state funding program of the North Carolina DOT, which is authorized under NC GS Chapter 63. The State Airport Aid Program funds both Safety/Regulatory/Operations projects and capital development projects.
Funding	AIP Funds – FAA
Eligibility	Regulatory projects include projects such as improving the condition of various pavements and the replacement of equipment such as lights or navigational aids. Capital development projects expand the airport for increasing capacity and/or alleviating congestion. Projects are processed and approved through the statewide Strategic Transportation Investments Program.
Source	https://connect.ncdot.gov/municipalities/State-Airport-Aid/Documents/2016_NC_Airport_PG_Handbook.pdf
Agency	NCDOT DoA
Program/Grant	NextGen Air Transportation (NGAT) Program
Purpose	To discover, evaluate, implement, and disseminate advanced air transportation technologies at the regional, national, and international level to improve the capacity, safety, and environment surrounding air transportation. NGAT is at the forefront of Unmanned Aerial Systems research and testing. NCDOT has provided labor and testing support to the NGAT Program to help meet Unmanned Aerial Systems user demand in North Carolina.
Funding	NCDOT DoA has partnered with the Institute for Transportation Research and Education (ITRE) at North Carolina State University to develop the NGAT Program.

Eligibility	There are no eligibility requirements.
Source	https://connect.ncdot.gov/municipalities/State-Airport-Aid/Documents/2016_NC_Airport_PG_Handbook.pdf https://connect.ncdot.gov/resources/Aviation%20Resources%20Documents/RP2015-16%20UAS%20Study%20Final%20Report.pdf
PENNSYLVANIA	
Agency	PennDoT
Program/Grant	Transportation Assistance Program
Purpose	Improving the state's aviation infrastructure
Funding	Projects receiving funding may receive up to 75% of the non-federal amount for federally eligible projects and a state reimbursement of up to 50% for non-federally eligible projects
Eligibility	Appropriately licensed public-use airports
Source	http://www.penndot.gov/Doing-Business/Aviation/AviationGrants/Pages/Aviation-Grant-Programs.aspx
TEXAS	
Agency	TxDOT
Program/Grant	2018 Routine Airport Maintenance Program (RAMP)
Purpose	Low-cost airside and landside airport improvements: These items can be more than just maintenance and may be new or additional items of work (e.g., construction of airport entrance roads, pavement of airport public parking lots, installation of security fencing, replacement of rotating beacon, etc.)
Funding	State funding is a $50,000 match per airport for each fiscal year. The state fiscal year begins September 1. The local government match is 50% of actual costs plus any in excess of $100,000 total costs.
Eligibility	Local governments can issue their own contracts for scope of services, or TxDOT local districts can perform services within their capabilities. TxDOT will not participate in contracts for any ineligible scope items or for costs that are unreasonable for the type of service. Local government force account work is NOT ELIGIBLE but purchase of materials for construction with sponsor labor is eligible.
Source	http://ftp.dot.state.tx.us/pub/txdot-info/avn/ramp_grants.pdf
VIRGINIA	
Agency	Virginia Dept. of Aviation
Program/Grant	State Entitlement Funds – Maintenance Program
Purpose	Sponsors of FAR Part 139 airports may use state entitlement funds to purchase maintenance equipment related to compliance with FAR Part 139 or to the safety and security of the airport. FAR Part 139 projects eligible for state participation are those directly related to meeting safety and performance standards established by FAR Part 139.
Funding	Sponsors may use state entitlement funds to secure maintenance contracts and repairs related to systems and equipment.

Eligibility	Elevators, escalators, security access systems, CCTV systems, terminal heating, ventilation and air conditioning systems, and systems not generally maintained by the airport personnel
Source	http://www.doav.virginia.gov/Downloads/Airport_Grant_Program/Airport%20Program%20Manual/2016%20Airport%20Program%20Manual/500%20DOAVAS%2020160819%202016%20Airport%20Program%20Manual%20bookmarked.pdf
WASHINGTON	
Agency	WSDOT
Program/Grant	Small Airport Fund (set asides from reduced entitlements for airports that collect PFCs)
Purpose	The state expects most funding to go through the AIP process and outstanding matched funds must be found by other sources and sponsors
Funding	This fund is split amongst: 1/7 (14%) – Small hub airports; 2/7 (29%) – GA airports; 4/7 (57%) – Non-hub primary and non-primary commercial service airports
Eligibility	There are no current eligibility requirements
Source	https://www.wsdot.wa.gov/NR/rdonlyres/765B30A4-8E34-457A-986E-DDFC13DFBDAF/0/3FundingAirportInvestments.pdf
Agency	WSDOT
Program/Grant	WSDOT's Airport Aid Grant Program
Purpose	The program provides crucial financial assistance to public-use airports in the preservation of Washington's system of airports.
Funding	The maximum amount WSDOT Aviation can award to an individual sponsor in a single grant is $750,000.
Eligibility	Any city, county, airport authority, political subdivision, federally recognized Indian tribe, public corporation, or person(s) that owns and operates a public-use airport included in the Washington Aviation System Plan is considered an eligible airport sponsor and may apply for WSDOT Airport Aid grant funds.
Source	https://www.wsdot.wa.gov/aviation/Grants/
Agency	WSDOT
Program/Grant	State Capital Improvement Program
Purpose	The State Capital Improvement Program tackles the challenge of targeting state and federal resources in a more strategic way by better identifying and prioritizing aviation-related projects.
Funding	The program is a continuous, multi-year funding program that will assess short-term (0-5 year) and long-term (5-20 year) airport improvement needs for the Washington state airport system.
Eligibility	Two Fronts: (1) A program for airports eligible for FAA AIP funds (2) A program for airports only eligible for WSDOT Airport Aid Program fund
Source	https://www.wsdot.wa.gov/aviation/Grants/SCIP.htm

APPENDIX H: ROM COSTING TABLE

(NOTE: Costs and time frames in Table H-1 are provided for example purposes only. Each SMPT will need to evaluate the actual planning, design, implementation costs, and time frames based on a specific airport and existing conditions.)

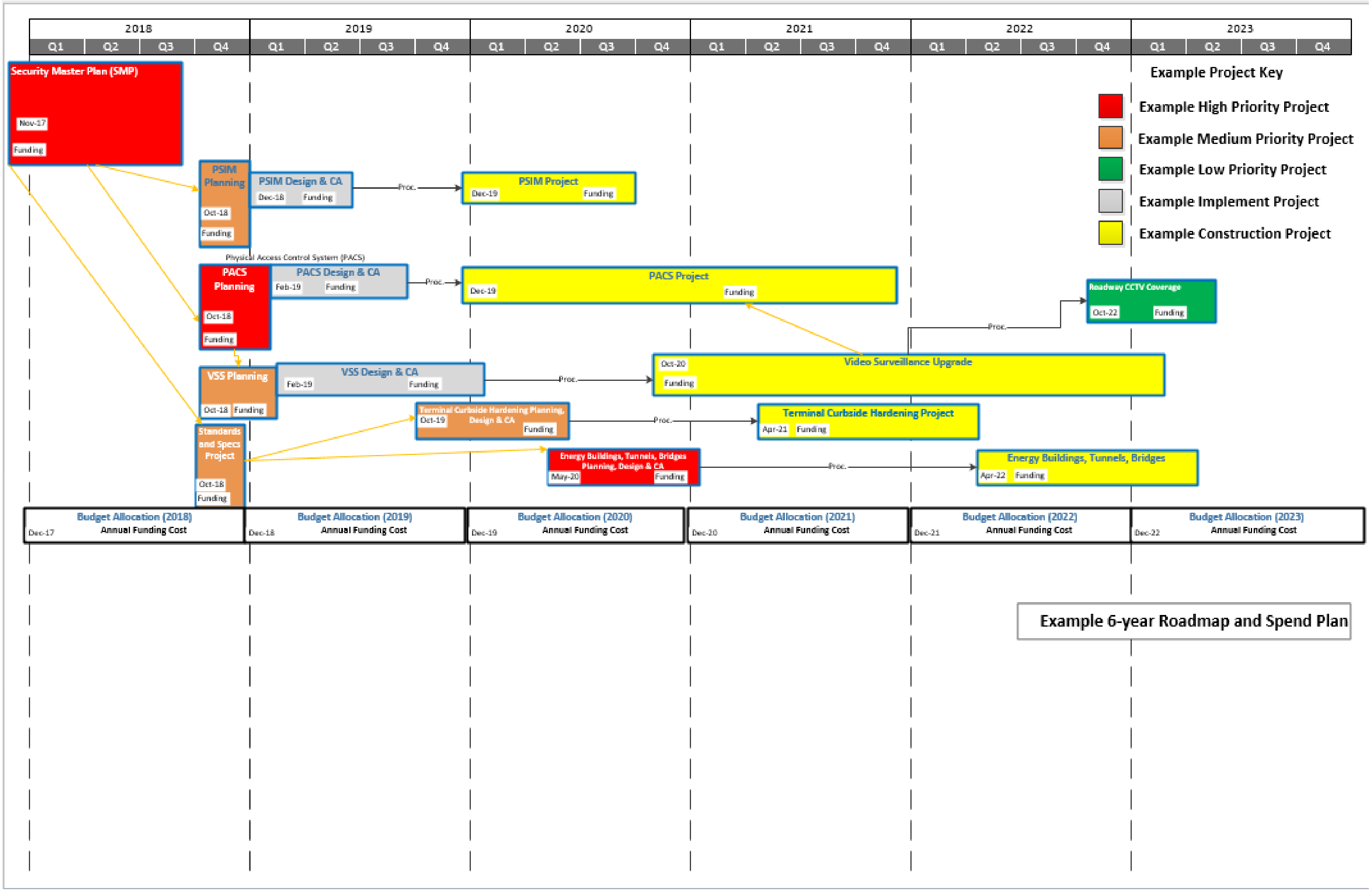
Table H-1. Example ROM Costing Table

ROM COST SUMMARY TABLE							
				ROM Cost			
Section	**Recommendation**	**Planning**	**Design Services**	**CA Services**	**Implementation**	**Total**	**Time Line Months**
9.3	Command, Control & Communication Systems Technology (PSIM)	$ 144,000	$ 336,000	$ 240,000	$ 4,800,000	$ 5,520,000	20
9.4	Physical Access Control System	$ 503,500	$ 1,174,877	$ 839,198	$ 16,783,950	$ 19,301,525	54
9.5	Video Surveillance System Upgrade	$ 627,844	$ 2,929,940	$ 2,092,814	$ 41,856,284	$ 47,506,882	60
9.6	Standard Security Boundary Design and Specifications	$ 75,000				$ 75,000	3
9.7	Barrier and Fence Upgrades	$ 13,200	$ 28,500	$ 9,250	$ 185,000	$ 235,950	9
9.8	Storm Drain Structure Security	$ 56,057	$ 130,799	$ 93,428	$ 1,868,552	$ 2,148,836	18
9.9	Perimeter Intrusion Detection System Development	$ 766,512	$ 1,788,528	$ 1,277,520	$ 25,550,400	$ 29,382,960	54
9.10	Gate Automation	$ 75,800	$ 206,232	$ 116,136	$ 2,322,721	$ 2,720,889	18
9.11	Gate Study, Gate Standards Development	$ 118,000				$ 118,000	6
9.12	Exit Only Gate Replacement and Upgrade	$ 46,320	$ 108,081	$ 77,201	$ 1,544,011	$ 1,775,613	18
9.13	Fuel Farm Security	$ 85,300	$ 199,035	$ 142,168	$ 2,843,355	$ 3,269,858	21
9.14	Terminal Curbside Hardenihng	$ 25,755	$ 60,095	$ 42,925	$ 858,500	$ 987,275	11
9.15	Tunnel Hardening	$ 23,850	$ 55,636	$ 39,740	$ 794,803	$ 914,029	15
9.16	Security of Remote Facilities	$ 150,000				$ 150,000	4
9.17	Security Enhancements	$ 20,000	$ 42,371	$ 30,265	$ 605,300	$ 697,936	17
9.18	Roadway CCTV Coverage	$ 120,000				$ 120,000	6
					TOTAL ROM COST	**$ 114,924,753**	

APPENDIX I: SMP 6-YEAR ROADMAP (EXAMPLE)

Figure I-1 is an example of an SMP (6-year) roadmap.

Figure I-1. Example 6-Year Roadmap with Spend Plan



APPENDIX J: SECURITY MASTER PLAN CHECKLIST

FIELD/QUESTION	RESPONSE(S)			
Conducted on	date			
Prepared by	prepared by			
Location	location			
Audit				
Scope and Strategy (Administrative)				
Precursor information needed to start a Security Master Plan is included in this "Administrative" section.				
Business Case & Scope Created?□ 1. Business case & scope template example provided in the PARAS0011 Appendices.	Yes, No, N/A	Note	Image	Action
Stakeholders Identified?		Note	Image	Action
Stakeholder Interviews Completed?□ (Sample questions provided in Section 5.2.1: Interviews)	Yes, No, N/A	Note	Image	Action
Security Subject Expert Engaged?	Yes, No, N/A	Note	Image	Action
Project Plan Created? 1. Project Plan template example available in the PARAS0011 Appendices.	Yes, No, N/A	Note	Image	Action
Define Scope	scope definition			
Benchmarking Completed? Benchmark elements: 1. Research airports in comparable hub size? 2. Benchmark on questions relevant to both physical and IT security? 3. Benchmark on questions relevant to airport funding mechanisms and strategies? 4. Benchmark on questions relevant to airport strategic initiatives and roadmaps for lifecycle replacement of security system elements? 5. Benchmark on questions relevant to the security element vendor technologies used (this to be used as a starting point for market research)? 6. Benchmark on questions relevant to internal staff count in IT and Security/Operations departments?	Yes, No, N/A	Note	Image	Action
Market Research Completed? 1. Identify vendors of security technologies used from benchmarked airports 2. Identify types of technologies and security systems to be potentially used at the airport (e.g., biometrics, network monitoring, drones, 360 degree cameras, video analytics, hard drive storage, etc.)	Yes, No, N/A	Note	Image	Action
Recent and/or historical assessments have been captured and documented? (Physical and cyber threat and vulnerability assessments, joint vulnerability assessments, DHS & CBP assessments, etc.)	Yes, No, N/A	Note	Image	Action
IT and Security Policies Reviewed? IT: 1. Computer and internet usage policy 2. Remote user access policy 3. Data retention and disposition policy 4. Data privacy policy 5. Network usage policy Security: 1. ID credentialing policy 2. Escort policy 3. Perimeter fencing maintenance policy 4. Physical infrastructure maintenance policy		Note	Image	Action
Existing airport projects vetted for dependencies and constraints pertaining to items in the Security Master Plan scope?	Yes, No, N/A	Note	Image	Action