PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0007 January 2018

Quick Guide for Airport Cybersecurity

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Synergy Solutions, Inc.
Oak Ridge, TN

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.

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 airport security technologies and procedures.

Through the Airport Security Systems 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 perimeter and access control security technologies and procedures.

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 0007 PROJECT PANEL

Royce Holden *Faith Group*
Xiaogong Lee *Ex Officio, Federal Aviation Administration*
Peter Longoria *Barich, Inc*
Susan Prediger *SP Consulting, LLC*
Lorena de Rodriguez *SSi, Inc*
Selena Tonti *Seattle-Tacoma International Airport*
Marci Woolson *CybrAnth*

CONTENTS

LIST OF FIGURES

SUMMARY

This Quick Guide is intended to help executives and managers at airports throughout the United States understand that they are accountable for cybersecurity issues and must measure and improve their cybersecurity programs and capabilities. It provides meaningful and actionable information for airport managers to evaluate and improve their own cybersecurity efforts. It also includes a series of detailed questions for an airport's Chief Executive Officer (CEO)/Director to ask their staff members about their airport's cybersecurity program. The assessment tool that accompanies this document measures the airport's cybersecurity risks and program maturity, and should be universally usable by large and small airports without additional software or hardware.

It is important to note that critical airport information systems addressed by this Guide and the accompanying assessment tool include high-end supercomputers and workstations, personal computers, tablets, and smart phones, as well as very specialized systems (e.g., customer-facing systems and services, telecommunications systems, industrial/process control systems, and environmental control systems). Modern airports cannot function without automation, and numerous threats exist to these systems, including purposeful attacks and defacement, environmental disruptions, and human or machine errors.

Leaders and managers at all levels must understand their responsibilities, and will ultimately be held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations. The purpose of this Guide and tool is to help them do so for the size of airport they operate.

PARAS ACRONYMS & ABBREVIATIONS

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

ACRP	Airport Cooperative Research Project
AIP	Airport Improvement Program
ANSI	American National Standards Institute
AOA	Air Operations Area
ARFF	Aircraft Rescue and Fire Fighting
CCTV	Closed Circuit Television
CDC	Centers for Disease Control and Prevention
CD/DVD	Compact Disc/Digital Video Disc
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
COO	Chief Operating Officer
DHS	Department of Homeland Security
DOT	Department of Transportation
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
ID	Identification
IED	Improvised Explosive Device
IP	Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
R&D	Research and Development
ROI	Return on Investment
SIDA	Security Identification Display Area

SOP	Standard Operating Procedure
SSI	Sensitive Security Information
SSN	Social Security Number
TCP/IP	Transmission Control Protocol/Internet Protocol
TSA	Transportation Security Administration
XML	Extensible Markup Language

SECTION 1: Introduction

1.1 Summary

This project was designed to produce a Quick Guide document and an automated Assessment Tool to assist airport management in identifying, assessing, and addressing risks in the operation of airport-managed information technology (IT) networks serving airport operations. These tools are intended to help airport management and technical staff assess the cybersecurity risks to their own networks and to help evaluate current and potential steps to mitigate these risks. The accompanying automated tool is applicable to airports of all sizes and complexities, and is aimed towards users with backgrounds in airport operations and general IT. This Quick Guide provides readers with a technical understanding of cybersecurity concepts, risks, and threats, as well as methods used to remediate various risks. It begins with a section specifically aimed at airport Director/CEO level executives to help them understand why cybersecurity is a serious issue, and methods to convey their needs to boards of directors and other oversight bodies.

The internet and its underlying infrastructure are vulnerable to a wide range of risks stemming from physical and cyber threats and hazards. Both sophisticated and novice cyber actors (i.e., hackers or other cyber criminals) exploit vulnerabilities to steal information and money, and disrupt, destroy, or threaten the delivery of essential services. Actors with little or no specific cyber knowledge can use widely available attack tools to cause significant disruption in an airport by disabling or interfering with automated processes and services such as baggage handling, electronic signage, heating and ventilation, automated parking services, and wireless networks.

> *A growing underground software industry for cyber-attack tools has developed, complete with technical support lines, money-back guarantees and testimonials from satisfied "customers."*
>
> *Source: Business Insider, Jan 5, 2016*

In addition to generalized cyber threats, the aviation sector remains a specific target for cyber actors.

Given the increasing potential for cyberattacks, it is important that airports be adequately prepared. For airports with limited IT technical or security resources, this includes meeting existing cyber threats, and continuing information exchange, training, and planning to meet new threats as they arise.

1.2 Objective

The objective of this project is to heighten awareness of cyber threats to ***airport managed information systems*** (as opposed to those managed and overseen by TSA or other entities), and to develop guidance to establish and/or enhance a cybersecurity posture for safe operations of airports. Airport Chief Information Officers, IT and cybersecurity managers, and all airport staff, tenants, and others, will find this Guide to be useful and applicable to their responsibilities at the airport.

This Guide offers the following:

- **Section 2:** Comprehensive tutorial specifically for the airport CEO and other senior executives
- **Section 3:** Brief explanation of the National Institute of Standards Cybersecurity Framework (NIST CSF), the methodology used in this Guide, and the accompanying assessment tool to evaluate the state of airport cybersecurity practices and the risks facing an airport (see also Appendix B of ACRP Report 140)

- **Section 4:** Step-by-step instructions for using the accompanying cybersecurity Assessment Tool to evaluate security risks associated with cyberspace—the tool offers a phased, prioritized approach to identifying risks and mitigations according to the individual needs and requirements of each airport
- **Section 5:** Compendium of successful best business practices for mitigating known threats and vulnerabilities, as well as maintaining security posture as threats and vulnerabilities evolve
- **Appendix A:** Comprehensive list of potential threats to airports
- **Appendix B:** List of relevant resources, as well as customizable presentations for use by airport operators to introduce the importance and applicability of cybersecurity
- **Appendix C:** Examples of questions a CEO should ask of his/her IT and cybersecurity staff
- **Appendix D:** General observations developed by the project team as a result of interviews conducted with a sample of airports around the country
- **Appendix E:** Notes on the roles and responsibilities of an organization's Chief Information Security Officer (CISO)

SECTION 2: For the Airport Executive

Airport CEOs and Directors are accustomed to being held accountable for what happens at their facilities. Although cybersecurity is often thought of as purely in the realm of technologists, it has become clear from press coverage, public reaction, legal cases, and legislative actions that CEOs and Directors will be held accountable for a major cybersecurity breach at their airports just as they would for a physical security breach or a serious aircraft accident.

This responsibility and accountability is equally true whether the airport is an international hub or a small community facility. The technology and IT security teams (employees or contractors) may be responsible for the day-to-day operational success or failure of airport cybersecurity, but the buck stops at the top. Unfortunately, one airport director interviewed by the project team summed up the prevailing attitude of many of his colleagues when he stated, "I don't really worry about this stuff… I have [the airport IT director] to handle that for me… I have bigger issues to deal with." The problem with this attitude is that if things go horribly wrong and the airport has a major cyber incident, the airport CEO is liable to be the one who suffers the most drastic and far-reaching repercussions, including possibly losing his or her job. Just as we have seen in the private sector when major cyber incidents occur, airport senior management could pay the ultimate career price in the aftermath.

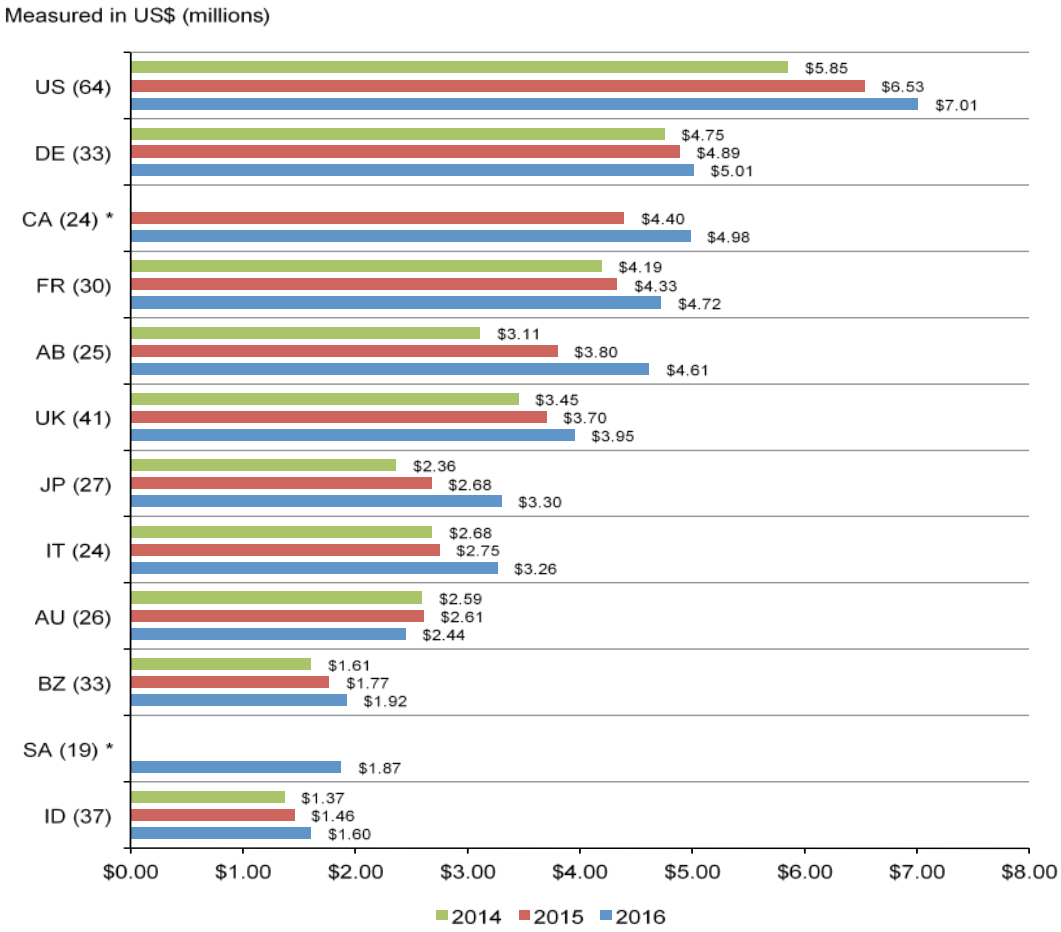
> *The median number of days an organization was compromised in 2015 before the organization discovered the breach (or was notified about it) was 146. In our experience, 146 days is at least 143 days too long.*
>
> *Source: Mandiant M-Trends 2016*

Information technology supports virtually all aspects of the operations of a modern airport, and similarly, a cybersecurity-related incident or breach that interrupts or degrades network operations will impact the operations of an airport in a myriad of ways. It can ultimately endanger the airport's ability to move passengers, cargo, or aircraft. In extreme cases, a severe interruption of services at an airport could cause a ripple effect that negatively impacts other airports and passengers throughout the system. In addition to traditional administrative processes such as human resources, payroll, finance, marketing, vendor services, email, badging, and access control, a severe cyber outage can disrupt building operations, baggage and cargo handling, electronic signage, parking operations, and airbridge operations. Less often considered but nevertheless vital controls such as energy management, sewage handling, heating, ventilation and air conditioning (HVAC), and people-moving capabilities can also be interrupted or damaged.

In addition to severe potential impact to airport operations and possible personal career damage, cyber incidents involve real and significant monetary costs. For example, according to a 2016 Ponemon Institute study, the total organizational cost of a typical cyber breach in the United States was estimated at $7 million per incident (see Figure 1 below). The same study found that the average cost of a compromised record from a data breach in the private sector in the United States was $158 per record. The cost of a single compromised record from a public-sector entity was much less, at $80, possibly because of the lack of alternatives to public services that precludes consumers from taking their business elsewhere after a breach.[1]

[1] *2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute, LLC, June 2016*

Figure 1. Total Organizational Cost of an Incident by Country – Ponemon Institute 2016



This section is dedicated to helping airport CEO/Directors and other senior executives responsible for the safe and secure operations of airports understand the cyber risks facing their airports and ways to counter those risks. The CEO's responsibility in addressing cyber threats is mainly to:

- Maintain an awareness of the threats and avoidable risks
- Be aware of inherent vulnerabilities of their IT infrastructures
- Understand the possible impacts and consequences of attacks against those infrastructures
- Balance cost and risk considerations in providing the maximum protection for the airport IT infrastructure and data
- Establish, maintain, and support the airport's "security culture" through personal example and allocating sufficient resources to security issues

The CEO must maintain a healthy and continual dialogue with the IT and cybersecurity staff of the airport, and ensure cybersecurity plans, controls, and assumptions are constantly assessed, tested, and exercised. The results of those activities must be communicated with all stakeholders and leadership and appropriately acted upon (see Appendix C for questions an airport CEO/Director should be asking his/her staff about the airport's cybersecurity program). Finally, and probably most importantly, the airport CEO/Director must set a leadership example by following the rules outlined in cybersecurity policy and by maintaining a constant organizational emphasis and focus on the airport's cybersecurity environment.

2.1 Cyber Risk Management

All airport senior leaders are comfortable with risk management; indeed, they weigh the cost of alleviating a given risk versus the likelihood of the risk occurring every day. To successfully protect an airport from cyberattack, cybersecurity risks must be added to the myriad of other risks (e.g., physical security breaches, aircraft incidents, public unrest due to noise complaints or changes in airport operations, etc.) that are addressed as part of an airport CEO's daily routine. Since a basic premise of risk management is that an organization cannot afford to eliminate all risks or stop all attacks, cyber risks must be included in the airport's comprehensive risk management program, and be given equal senior management consideration with financial, operational, reputational, and other risks the airport faces.

This Guide places cybersecurity into the broader organizational context of successfully operating an airport. The premise is simple: *Failure to give adequate senior executive attention to airport cyber risk and cybersecurity will eventually result in serious and costly impact to airport services and reputation, and perhaps career-ending consequences for the airport's senior executives.*

Effectively managing cybersecurity risk organization-wide requires the following key elements:

- Ongoing recognition and understanding by senior leaders of the cybersecurity threats and risks to airport operations
- Establishing a clear tolerance level for risk and communicating that risk tolerance throughout the organization
- Establishing and communicating accountability by senior leaders and executives for their risk management decisions

2.2 Threats to Airports

The motives of cyber attackers generally fall into four general categories, all of which can reduce an airport's ability to serve the community and provide service to passengers.

2.2.1 Political or Military

The most serious and significant sources of attack are conducted by foreign military or intelligence-related sources. These attackers are usually attempting to gain some military, political, or strategic insight, and will attack the availability and integrity of systems to undermine the trust of the public or leaders. Although there are notable recent exceptions, such as the alleged hack of Sony Pictures by the North Korean government in 2014, these attackers usually target military organizations, government agencies, or related public or private non-governmental organizations to compromise and disrupt their operations or steal information. As part of the nation's critical infrastructure, airports are highly symbolic and practical targets for possible attacks of this type. Disruption of air travel at key airports could cause system-wide service disruptions and critically damage public trust and confidence in the entire National Airspace System.

2.2.2 Commercial Espionage

Attackers with this motivation are usually aligned with sophisticated organized cybercrime entities, or foreign governments that wish to steal or damage confidential or proprietary information from private and public companies. This type of attacker often seeks significant monetary gain, or social activist or

corporate strategic goals. Airport planning, construction, budget, and public- or government-relations documents are examples of tempting targets for attackers intent on commercial espionage.

2.2.3 Disruption

A wide variety of individuals and groups engage in cyberattacks aimed at disrupting or disabling access to resources. They carry out their attacks for a range of reasons—from political protest and attempts at economic harm to simple amusement or to gain status within their peer group. These attacks are most often conducted by vandals, activists, or outsiders with an overarching agenda. They usually target networks or systems to deny user access, inflict damage, or steal or corrupt data. An example of this type of attack in the airport environment would be an attacker who attempts to prevent access to the airport website by flooding the site with more traffic than the site can handle (i.e., a distributed denial-of-service or DDoS attack). Another example would be an attacker, seeking to expose perceived wrongdoing by airport management, who steals and publishes the contents of airport management email and executives' personal information on a site such as WikiLeaks.

2.2.4 Cybercrime

Cybercrime is perhaps one of the most rapidly growing areas of attack activity. These attacks are often less sophisticated than the other types of attacks discussed above, but over the last few years, cybercrime techniques and tools have improved and become much easier to obtain and use. These attackers usually target networks and systems directly for data they can steal and resell, such as customer identification, credit card, or banking information. Also, by using ransomware or destructive malware, actors can encrypt or destroy data, or threaten exposure of sensitive communications and information unless the victim pays a fee. Airport systems that handle credit card information parking services or baggage fees would be prime targets for these attackers.

2.2.5 Possible Impacts on Airport Operation

As is the case in most other large organizations, the possible types and impacts of cyberattacks on an airport are limited only by the imagination of the attacker and his or her ability to gain access to carry out an attack. As noted above, virtually all operations of a modern airport depend on IT connectivity and the airport network in some manner. Significantly, this includes functions far beyond the traditional administrative activities to the stability and well-being of the basic environmental and operational processes that allow the airport to function at all. The list shown below of ways actors might impact an airport is meant to be only illustrative and not exhaustive; attackers have proven to be extremely imaginative and persistent in devising new and unique attacks and outcomes to impact their victims. Appendix A to this Guide contains a more comprehensive list of threats, many of which would be applicable to the airport environment if undertaken by an imaginative attacker.

- Attacks on electronic signage to disable signs or change content
- Ransomware on airport, airline, or vendor systems
- Baggage system disruptions or misconfiguration
- Interruptions to HVAC, electricity, or other building functions
- Parking system issues
- Credit or debit card data theft

- Theft of sensitive emails or documents to blackmail or embarrass airport management or other parties
- Defacement of airport websites
- Attacks on badging or access control systems
- Disruption of jetway or other ramp functions
- Attacks to prevent access to airport networks
- Release of airport executive's personal information, such as address, phone number, family members, etc. (a.k.a. "doxing")
- Establishing a fake airport website to spread misinformation or gather personal information
- Disruption of airport systems via malware delivered via phishing emails
- Attempts to access physical security systems
- Unauthorized access to sensitive files

SECTION 3: Cybersecurity Basics and the NIST Cybersecurity Framework

Just as a plan is necessary when you build a new house, a blueprint is required to build and maintain a good cybersecurity program. These blueprints or frameworks are used to outline the various processes, activities, technologies, and policies that should be present to provide an adequate cybersecurity structure. The framework referenced in this Quick Guide and the accompanying assessment tool is based on the NIST Cybersecurity Framework (CSF).

3.1 Framework Organization

The NIST CSF is organized around five essential functions that must be carried out in any cybersecurity program. These functions are:

- **Identify** your important assets, data, elements of risk, and vulnerabilities
- **Protect** yourself through technical tools, policy, or personnel-related methods
- **Detect** attempts to attack your network or data rapidly using various tools and techniques
- **Respond** to those attempts to counter the attack and contain any damage
- **Recover** to a pre-event state and use lessons learned from the incident to improve the process

These functions interact and support each other and should all be addressed in an airport's cybersecurity program (see Figure 2). Each function will be discussed in more depth below.

Figure 2. Functions of the NIST Cybersecurity Framework

3.1.1 Identify

To protect your airport's IT infrastructure, you must have a clear understanding of what it is you are protecting, its value, and criticality if lost, destroyed, or disrupted. In addition, you need to have a keen understanding of the risks, threats, and vulnerabilities faced by your airport IT infrastructure. This function covers several critical areas including the way you identify and maintain the hardware, software, and data assets your airport uses to operate, and your airport's business environment, governance, and risk management strategy and processes.

3.1.2 Protect

Possibly one of the most dynamic and volatile areas of cybersecurity is the way people, processes, and technology assets are employed to protect cyber infrastructures. The Protect function of the NIST CSF examines the tools, techniques, and policies the airport has employed in its cybersecurity program. Areas examined include IT Network and Device Access Control**,** Cybersecurity Awareness and Training**,** Data Security**,** Operational Processes and Procedures, Maintenance, and Protective Technology.

3.1.3 Detect

One of the keys to an effective and successful cybersecurity program is the ability to effectively monitor network and device operations, and quickly and accurately detect, identify, analyze, categorize, and validate suspicious events. In conducting a detailed examination of the various functions and tools used to detect suspicious actions on networks and devices at the airport, the NIST CSF reviews three areas: Detecting Anomalies and Events, Continuous Monitoring for Security, and Detection Processes.

3.1.4 Respond

Studies have shown that timely response to a cyber incident is key to minimizing damage, data loss, and other negative consequences of a cyberattack or incident. Unfortunately, other studies indicate that the average successful cyberattack goes unrecognized by victims for an average of 146 days (almost 5 months).[2] When cybersecurity events or incidents occur, airport management must respond quickly and effectively to identify the issue, analyze and investigate it, and remediate or contain the damage. The NIST CSF examines five areas in this section: Planning for Response, Communicating during an Incident, Situation Analysis, Mitigation of Vulnerabilities and Response Plan Improvement.

3.1.5 Recover

After a cybersecurity incident has been fully investigated and the underlying vulnerabilities remediated, a separate process of recovery to the pre-incident state is necessary. This section looks at three areas: Planning for Recovery, Improvements to Recovery Plans, and Communications.

By using a framework such as the NIST CSF as the outline for a cybersecurity program, an airport can ensure it has a comprehensive approach to evaluating cyber risk and effectively managing that risk.

2 *M-Trends 2016, Mandiant Consulting, FireEye, https://www.fireeye.com/blog/executive-perspective/2016/02/m-trends_2016.html*

SECTION 4: Risk Assessment Tool

In order for an airport staff to assess their own specific risk environment and cybersecurity program, this Quick Guide is accompanied by a Cybersecurity Risk Assessment Tool. The tool is written in widely available software (Microsoft Excel and Microsoft Visual Basic) to allow maximum ease of use without having to install special programs or buy additional equipment. The tool is meant to be used by airport operations and IT staff at airports of any size or operating structure. Using the tool, staff members can perform a basic step-by-step assessment of the risks airports face by simply being open for business, as well as a longer assessment that examines the airport's current cybersecurity practices, policies, and technologies. The tool provides management-level reports in several formats (e.g., printed, PDF, etc.) to allow airport executive management to identify unaddressed areas of risk and sections of their cybersecurity program that need attention.

The tool is designed to assist airport management in identifying, assessing, and addressing risks in the operation of airport-managed IT networks serving airport operations. Using the tool, airport operations and technical staff can assess the cybersecurity risks to their own IT systems and networks, evaluate their current cybersecurity program efforts, and identify potential steps to mitigate the risks that still exist. The tool is designed to be applicable to airports of all sizes and complexities, and is meant to be used by persons with backgrounds in IT and airport operations. The tool is organized around the structure of the NIST Cybersecurity Framework, as explained in the previous section of this Guide. The questions used in the tool should be self-explanatory, but a glossary is provided for unfamiliar technical terms users might encounter.

This portion of the Quick Guide document provides an overview of the underlying philosophy of the tool, as well as providing detailed instructions on how to use it and interpret its results.

4.1 How the Tool is Organized

The Cybersecurity Risk Assessment Tool is organized around two basic questions faced by airport executives:

1. What are the cybersecurity risks my airport faces?
2. How effective are our current cybersecurity efforts and how can they be improved?

To help answer these questions, the tool is similarly organized into two main sections:

- Inherent Risk Assessment (measuring airport cybersecurity risk)
- Cybersecurity Risk Assessment (measuring cybersecurity program effectiveness and maturity)

4.2 How the Tool Works

The tool develops risk and cybersecurity program maturity ratings using a series of multiple-choice questions about the airport, its operating environment, services it provides customers and employees, how it is governed, and the cybersecurity program steps currently in place. Staff members utilizing the tool need not be cybersecurity experts; it is designed to be usable by staff with airport operations and general IT backgrounds. While having someone with cybersecurity experience and training on the team will be helpful in some cases, it is not a requirement.

As the airport team answers the questions in the tool, numeric values are assigned to the answers chosen. The accumulated values are used to determine relative risk or maturity scores, depending on the section of the tool being used. Reporting for both sections (Inherent Risk and Cybersecurity Risk) is performed when the tool is completed. Instructions for using the tool are provided below.

4.2.1 The Home Screen

When the tool is executed, the user first sees a screen that introduces the tool and offers a brief explanation on how it is organized and operates. The two main sections of the tool are readily apparent on the home screen (Figures 3 and 4) and are labeled Inherent Risk Profile and Cybersecurity Risk. Each of these sections are further divided into subsections to allow the user to easily navigate around the tool.

When using the tool for the first time, users should click on the button to reset the answers in both sections of the tool. This will initialize the tool and clear out any answers remaining from previous users. Each major section of the tool (i.e., Inherent Risk Profile and Cybersecurity Risk) is meant to stand alone, and no data is passed from one section to the other. However, most airport users will find it easiest to complete the Inherent Risk Profile section first to understand some of the risks facing their airport and to gain familiarity with tool functionality.

Figure 3. Cybersecurity Assessment Tool Home Screen Inherent Risk Profile Section

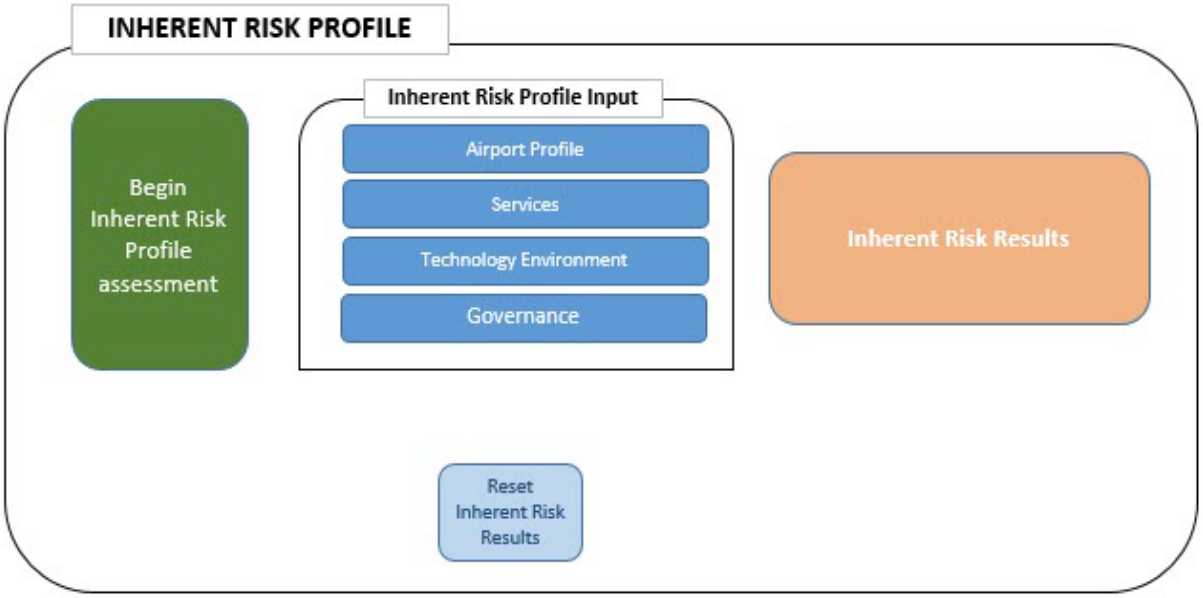
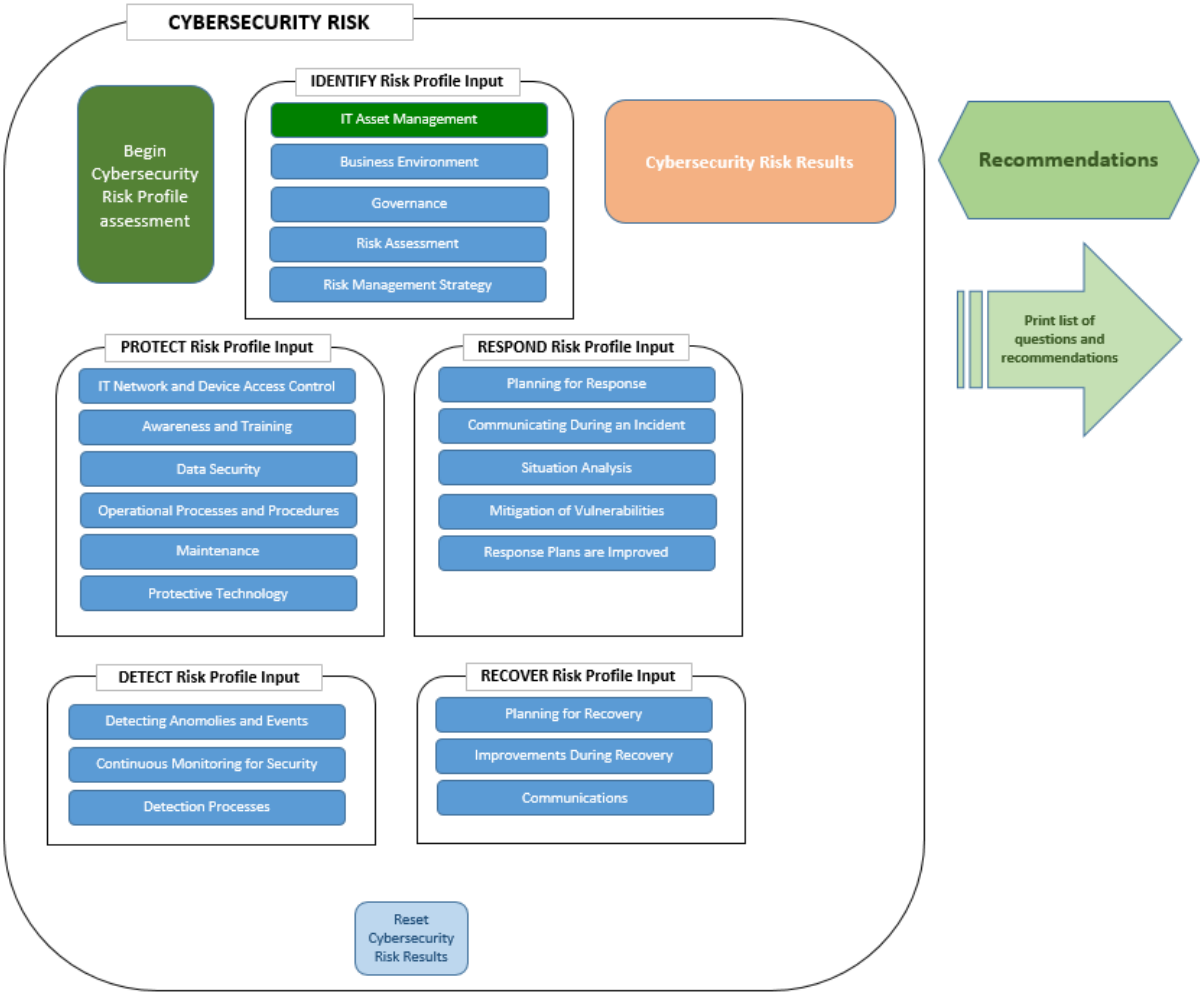


Figure 4. Cybersecurity Assessment Tool Home Screen (Cybersecurity Risk Section)



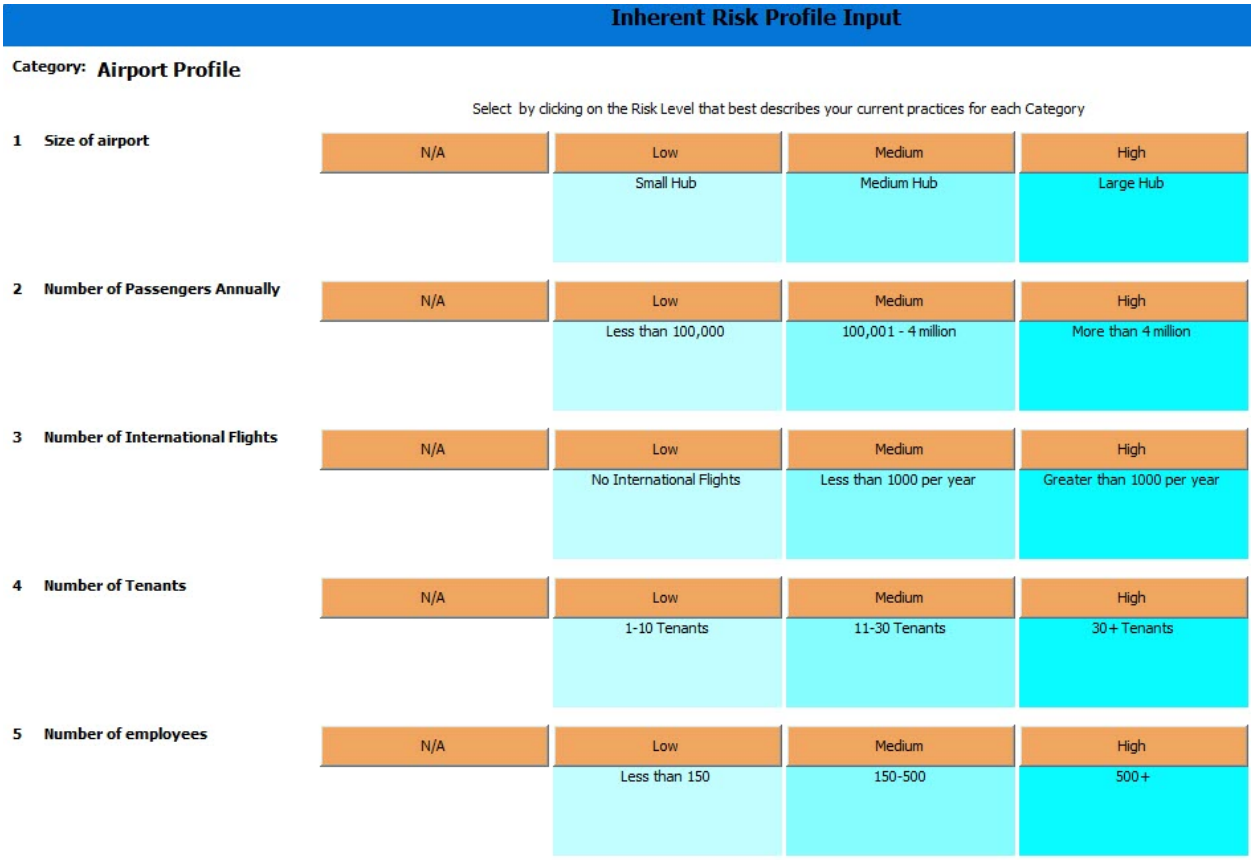
4.2.2 Inherent Risk Profile Section

The Inherent Risk Profile section (Figure 3) uses a series of questions in four areas to develop a simple estimate of the airport's risk environment: (1) the airport profile, (2) services offered to passengers and staff, (3) the airport's technology environment, and (4) the governance environment of the airport. To begin using the tool, the user clicks on the green Begin Inherent Risk Profile Assessment button. Subsequently, for each section of the assessment, a series of questions are asked and three possible answers representing low, medium, and high-risk conditions are presented. The user selects the answers that ***most closely correspond*** to their specific airport environment. When a button is selected by the user, the button color changes from orange to green. If none of the three answers are applicable to the airport, the user can click on the button marked N/A and that answer will be excluded from consideration when risk scoring is performed. The user continues to answer the risk-related questions until all are answered (see Figure 5 for an example of the Inherent Risk Profile questions).

A comments section is provided for each question to allow the user to record explanatory notes or comments. These comments are included in the outputs generated by the tool's reporting function.

If the user needs to return to a previous answer, Previous and Next buttons at the bottom of each page of questions allows navigation within that section. All questions on a given page must be answered before the tool will allow the user to continue to the next page of questions. The tool automatically progresses through all the subsections of the Inherent Risk Assessment and produces a summary report (Figure 6) after the final question is answered. The tool automatically saves the answers for unfinished assessments, so users can leave the tool and return later to resume the assessment.

Figure 5. Example of Inherent Risk Profile Questions



Inherent Risk Profile Input

Category: Airport Profile

Select by clicking on the Risk Level that best describes your current practices for each Category

		N/A	Low	Medium	High
1	**Size of airport**		Small Hub	Medium Hub	Large Hub
2	**Number of Passengers Annually**	N/A	Low Less than 100,000	Medium 100,001 - 4 million	High More than 4 million
3	**Number of International Flights**	N/A	Low No International Flights	Medium Less than 1000 per year	High Greater than 1000 per year
4	**Number of Tenants**	N/A	Low 1-10 Tenants	Medium 11-30 Tenants	High 30+ Tenants
5	**Number of employees**	N/A	Low Less than 150	Medium 150-500	High 500+

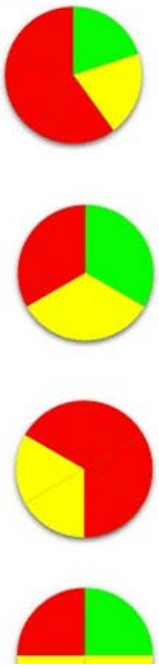
Figure 6. Summary Report for Inherent Risk Profile

Inherent Risk Results

Notes | Save | Send Mail | Print

Summary Results of Inherent Risk Profile:

Inherent Risk Profile Input	Risk Level	Risk Score (Range 1 – 5)
1. AIRPORT PROFILE	**Medium**	**3.8**
1.a. Size of Airport	Low	1
1.b. Number of Passengers Annually	Medium	3
1.c. Number of International Flights	High	5
1.d. Numbers of Tenants	High	5
1.e. Number of Employees	High	5
2. SERVICES	**Medium**	**3**
2.a. Wifi for Passengers?	Low	1
2.b. Wifi for Employees?	Medium	3
2.c. Wifi for Tenants?	High	5
3. TECHNOLOGY ENVIRONMENT	**High**	**4.3**
3.a. Website?	High	5
3.b. Application Environment	High	5
3.c. Common Use Network?	High	5
3.d. Technology Environment Outsourced?	Medium	3
3.e. Technology Asset Management	Medium	3
3.f. Mobile Devices (phones, tablets, etc.)	High	5
4. GOVERNANCE	**Medium**	**3**
4.a. Airport Governance Model	Low	1
4.b. Cybersecurity Plans and Policies	Medium	3
4.c. Cybersecurity Training	Medium	3



4.2.3 Inherent Risk Calculation and Reporting

When all the questions are answered in the Inherent Risk Profile section of the tool, a summary report is displayed that provides a numeric risk score and a descriptive rating for each of the specific areas of risk (i.e., Airport Profile, Services, Technology Environment, and Governance) as well as ratings for individual subareas of each. The report can also be viewed at any time while using the tool by clicking on the orange Inherent Risk Results button on the tool Home Page.

The numeric ratings are computed by assigning a point score to each of the questions (*Low Risk* = 1 point, *Medium Risk* = 3 points and *High Risk* = 5 points). Answers of N/A get zero points; when the Inherent Risk Score is derived from an average taken from the total number of points in a section, this has the effect of lowering the overall risk score for that section and subsection of the tool. If a risk factor is not present (e.g., there is no wireless access for airport customers and vendors) and results in an N/A to be selected, then this will lower the overall risk to the airport because that area of threat is not present. Points are added for each area and subarea to develop a cumulative Risk Score. Throughout the Inherent Risk Profile section, a total risk score of 0–1.99 points generates a Risk Rating of Low, a score of 2–3.99 points generates a Risk Rating of Medium, and a score of 4–5 points generates a High Risk Rating.

The summary report produced for the Inherent Risk Profile section of the tool (Figure 6) lists both the Risk Score and a Risk Level for each subsection of the profile, as well as for each of the individual sections (Low Risk is labeled in green, Medium Risk is labeled in yellow, and High Risk is labeled in

red). In addition, simple pie charts using the same color codes provide an at-a-glance representation of how the airport's risks are distributed.

The Send Mail button can be used to send a copy of the report to other airport team members and the Print button can be used to print the report or convert it to a PDF using the Microsoft Office Print to PDF function. *(Note: Due to program limitations, the Send Mail function can be used only on systems where Microsoft Outlook is installed.)* Comments can be added to the report in the Notes box provided and saved using the Save button.

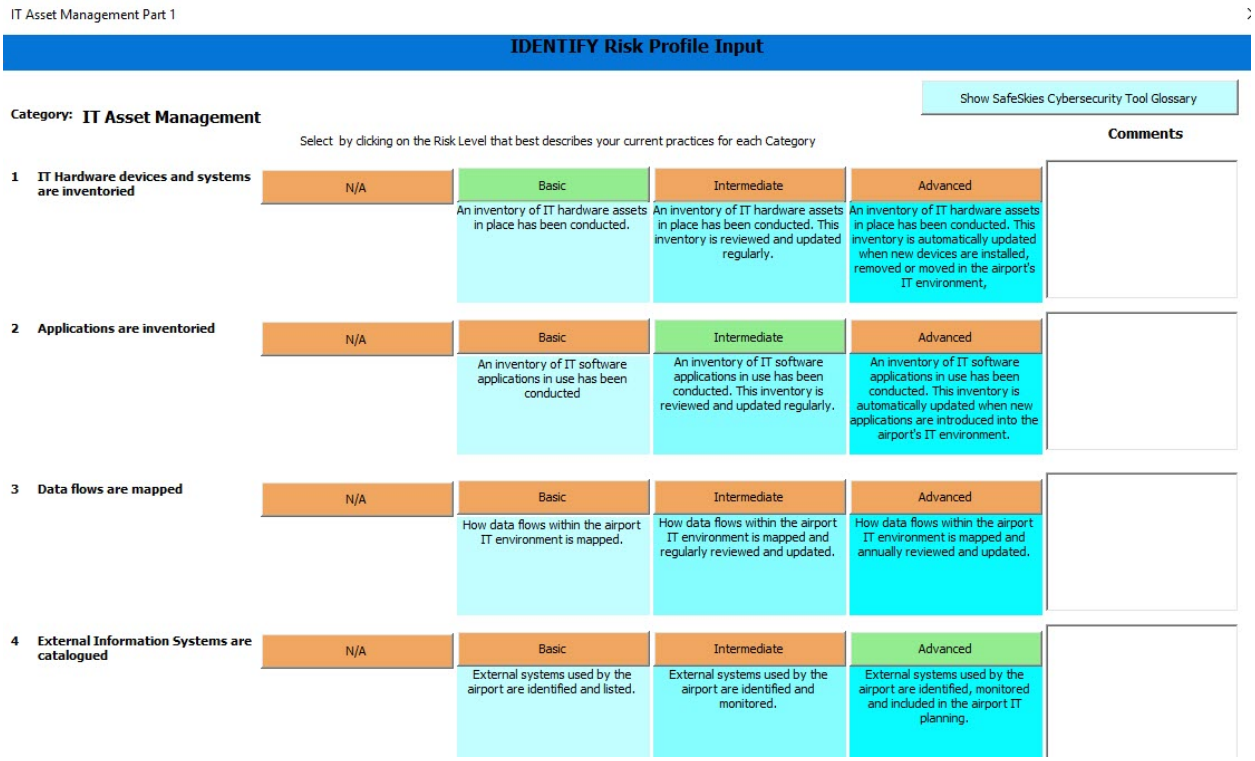
Using this report, airport management can identify and review individual areas of risk and determine if mitigation actions are needed. Management may also want to include specific risk goals for their staff as part of their overall risk management program. For example, a goal to have no High Risk items identified in the tool might be established for staff to work towards.

4.2.4 Cybersecurity Risk Section

The Cybersecurity Risk section of the tool is organized around the sections and subsections defined in the NIST CSF. The main sections of this framework (i.e., Identify, Protect, Respond, Detect, and Recover) correspond to the primary sections of the NIST CSF as discussed in Section 3 of this Quick Guide. Likewise, the 22 subsections in the tool correspond to similarly named subsections of the NIST CSF (see Figure 4).

This section of the tool develops a rough cybersecurity program maturity score based on the airport team's answers to a series of descriptive multiple-choice questions. The maturity score is converted to a maturity label, which describes the airport cybersecurity program as being Basic, Intermediate, or Advanced. As in the Inherent Risk Profile section of the tool, users are expected to click on the answer that ***most closely describes*** their particular cybersecurity situation. If none of the three selections applies to the airport, the users should again select the N/A answer. In this section of the tool, selection of an N/A answer for a specific question contributes zero points to the cybersecurity maturity score. Because the cybersecurity maturity score is derived from an average of the point total, an N/A answer has the effect of lowering the overall maturity score for that section and subsection of the tool.

Figure 7. Example Cybersecurity Risk Questions



4.2.5 Entering Cybersecurity Risk Section Data

As with the previous section of the tool, before a user first enters their own answers, answers from previous users should be cleared by clicking on the blue button labeled Reset Cybersecurity Risk Results. To begin using the tool, users should click on the green Begin Cybersecurity Risk Profile Assessment button and start answering the questions in the various subsections (see Figure 7 for sample questions). Again, users should pick the answers that most closely describe their airport's cybersecurity program. The answers in the tool are categorized as being indicative of Basic, Intermediate, or Advanced maturity levels.

When an answer is chosen, a point value is assigned to it based on the maturity level of the answer. A Basic level answer receives 1 point, an Intermediate level answer receives 3 points, and an Advanced level answer receives 5 points. Points are averaged for each of the subsections to determine a maturity level rating for that subsection. An average of 0–1.99 points results in a Basic maturity level for that subsection, 2–3.99 points results in a maturity level of Intermediate, and an average of 4–5 points results in an Advanced maturity level. Although the tool has been written to be understandable by non-technical users, some terms that are unique to cybersecurity are used in the questions. Users who are unsure of a term's meaning can click on the button labeled Show Safe Skies Cybersecurity Tool Glossary that is in the top right of every questions screen, which will direct them to a glossary with basic definitions. A comments section is provided for each question for users to enter comments, explanatory notes, or questions. The content of the comments section is printed in the reporting of the tool.

Figure 8. Cybersecurity Risk Report

Cybersecurity Risk Results

Notes Save

Send Mail Print

Summary Results of the Cybersecurity Risk Profile:

Cybersecurity Risk Profile	Risk Level	Risk Score (Range 1 – 5)
1. IDENTIFY	**INTERMEDIATE**	**2.7**
1.a. IT Asset	Intermediate	3.7
1.b. Business	Basic	1
1.c. Governance	Basic	1.5
1.d. Risk	Intermediate	3.7
1.e. Risk	Intermediate	2.3
2. PROTECT	**INTERMEDIATE**	**3.5**
2.a. IT Network and	Intermediate	2.6
2.b. Awareness	Intermediate	2.3
2.c. Data Security	Intermediate	2.2
2.d. Operational	Intermediate	3.4
2.e. Maintenance	Advanced	4
2.f. Protective	Intermediate	3.4
3. DETECT	**INTERMEDIATE**	**3.2**
3.a. Detecting	Intermediate	3.4
3.b. Continuous	Intermediate	2.8
3.c. Detection	Intermediate	2.3
4. RESPOND	**INTERMEDIATE**	**3.3**
4.a. Planning	Advanced	5
4.b. Communicating	Intermediate	2.6
4.c. Situation Analysis	Intermediate	3
4.d. Mitigation of	Intermediate	3
4.e. Response	Intermediate	2

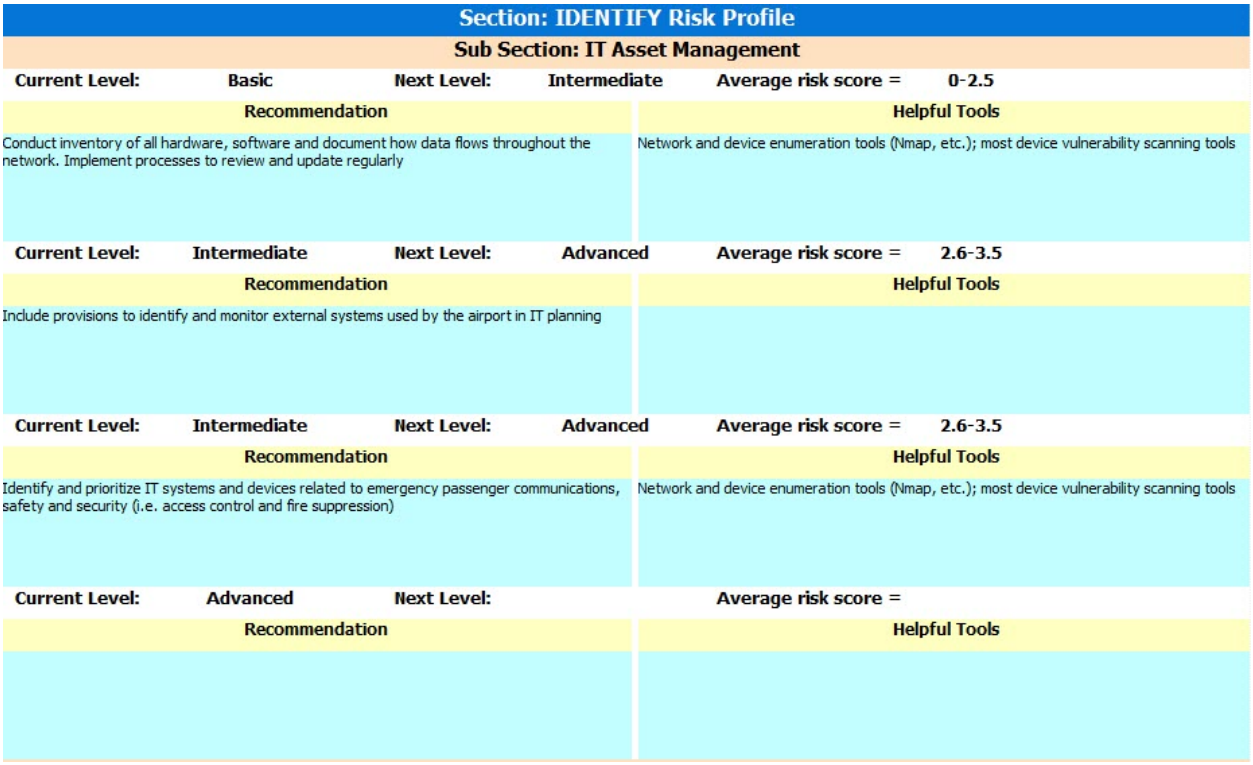
4.2.6 Reporting

Once users have answered all questions in the Cybersecurity Risk section of the tool, a summary report is displayed. This report gives an overall cybersecurity maturity rating and score for the program, as well as ratings and scores for individual subsections (Figure 8). As before, color coding is used for Basic (red), Intermediate (yellow) and Advanced (green) maturity ratings in both the labels used in the individual section ratings and the pie charts showing the distribution of ratings in the tool. A summary report can be generated by pressing the orange Cybersecurity Risk Results button on the Home Page at any point during the time a user is entering data into the tool.

In addition to producing a summary report, the tool also produces a recommendations report that is designed to provide suggestions to management for improving the maturity rating for a given subsection. Users are provided recommended actions for improvement, and examples of helpful tools that are available for little or no cost online are given where appropriate (see Figure 9 for an example of the recommendations report).

Reports can be printed or converted to a PDF by clicking on the Print button provided, or be emailed to other airport staff as described above.

Figure 9. Sample Recommendations Page



Section: IDENTIFY Risk Profile					
Sub Section: IT Asset Management					
Current Level:	**Basic**	**Next Level:**	**Intermediate**	**Average risk score =**	**0-2.5**
Recommendation				**Helpful Tools**	
Conduct inventory of all hardware, software and document how data flows throughout the network. Implement processes to review and update regularly				Network and device enumeration tools (Nmap, etc.); most device vulnerability scanning tools	
Current Level:	**Intermediate**	**Next Level:**	**Advanced**	**Average risk score =**	**2.6-3.5**
Recommendation				**Helpful Tools**	
Include provisions to identify and monitor external systems used by the airport in IT planning					
Current Level:	**Intermediate**	**Next Level:**	**Advanced**	**Average risk score =**	**2.6-3.5**
Recommendation				**Helpful Tools**	
Identify and prioritize IT systems and devices related to emergency passenger communications, safety and security (i.e. access control and fire suppression)				Network and device enumeration tools (Nmap, etc.); most device vulnerability scanning tools	
Current Level:	**Advanced**	**Next Level:**		**Average risk score =**	
Recommendation				**Helpful Tools**	

In addition to the recommendations report, a report of assessment questions and the answers entered can also be produced by clicking on the arrow on the Home Page.

SECTION 5: Cybersecurity Best Practices

This section provides successful best business practices (at the time of publication) for identifying and mitigating known threats and vulnerabilities, and maintaining security posture as threats and vulnerabilities evolve.

For example, airport executives and management may have questions regarding cybersecurity and airport operations such as, how would their team respond if the local Wi-Fi system were compromised? What negative public perception might this have on an airport when passengers cannot access e-ticketing airline partner applications? How would this affect ramp operations? How would concessionaires react? Would airline stakeholders be affected by loss of service?

On a larger scale, what if the supervisory control and data acquisition (SCADA) systems were disabled and baggage control systems, runway lighting, and energy supply management were affected? In this scenario, it is difficult to foresee any other outcome outside of severely degraded operations or outright airport closure. What steps do airport operators need to take to ensure that the airport is adequately protected against the threat of a cyberattack? Some answers might include:

- Conducting periodic risk assessments
- Ensuring plans, policies, and procedures are current, and ensuring the staff complies with them—this includes signed cybersecurity acknowledgements by all system users
- Improving cybersecurity operations
- Expanding cybersecurity education and training programs for employees, partners, and possibly passengers
- Conducting frequent and extensive network penetration testing, application vulnerability tests, and tabletop exercises

5.1 Best Practices Identified in ACRP Report 140

The following list provides 11 best practices as stated in ACRP Report 140:

1. Become and stay aware of the threats that can impact critical data and systems by maintaining regular communication with peers and related agencies, participating in information sharing forums, and engaging (if the means exist) cybersecurity professionals.
2. Establish and enforce policies for acceptable use, sensitive security information (SSI), information privacy, software and data assurance, training, and communications.
3. Periodically train managers, staff, consultants, and tenants on their roles to protect data and system credentials, to be wary of social engineering tactics, to adequately protect the devices they control, and to report suspicious activity and policy infractions. Update this training as new threats emerge.
4. Maintain an inventory of data, systems, network devices, and users that may be affected by a cyberattack. Understand how data flows within your network and keep current network architecture diagrams describing your network.
5. Identify vulnerabilities where these assets are not adequately protected, and prioritize them based on the impact a successful attack may have. Periodically scan applications, websites, and devices for vulnerabilities.
6. Implement countermeasures to achieve the level of protection that is desired and affordable.

7. Assign CISO responsibilities to a qualified staff member, new hire, or consultant. (See Appendix E for a list of typical duties and responsibilities of a CISO.)
8. Monitor computer and human behavior through manual and automated means.
9. Communicate anomalous activity and successful attacks to the CISO, IT staff, senior management, affected stakeholders, other agencies, and law enforcement personnel.
10. Be prepared to isolate affected systems, remove them, recover from attacks, and learn from them.
11. Recognize that, even if all the foregoing measures are implemented, the airport will still not be fully protected. Remain vigilant and continuously improve the level of protection to the extent possible given the available resources.

GLOSSARY, ABBREVIATIONS, AND ACRONYMS

Actor	An individual or group that can manifest a threat
Cyberattack	A deliberate attempt to violate the security of a digital system. A successful attack is one that achieves its goal, typically causing harm to information, systems, or infrastructure or disrupting operations that rely on these resources.
Cybersecurity	Means and methods that protect data and systems from unauthorized access, inappropriate modification, or unintentional loss.
Industrial Control Systems (ICS)	Information systems used to control industrial processes such as manufacturing, product handling, production, and distribution. ICS include SCADA systems used to control geographically dispersed assets as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes (Joint Task Force Transformation Initiative 2012).
Motive	Something that causes a person to act (Merriam-Webster 2014).
Target	The data or system to which an actor wishes to gain access.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service (Committee on National Security Systems 2010).
Vulnerability	A weakness that exposes data and/or systems to threat. Vulnerability is introduced by the lack of countermeasures to adequately protect an asset (Committee on National Security Systems 2010).

A-ISAC	Aviation Information Sharing and Analysis Center
BYOD	Bring Your Own Device
CISO	Chief Information Security Officer
DDoS	Distributed Denial of Service
HIPAA	Health Insurance Portability and Accountability Act
HVAC	Heating, Ventilation, and Air Conditioning
ICS	Industrial Control Systems
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
MS-ISAC	Multi-State Information Sharing and Analysis Center
PCI	Payment Card Industry
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition

APPENDIX A: **Cyber Threats**

The chart below gives an extensive list of possible threats to a given organization that may be applicable to the airport environment. Given the adaptability and imagination displayed by many attackers, this should be considered food for thought and not an exhaustive list. (Source: *NIST Special Publication 800-30, Guide for Conducting Risk Assessments, Appendix E, National Institute of Standards and Technology, September 2012, Washington, D.C.*)

Threat Events (Characterized by TTPs)	Description
Perform reconnaissance and gather information	
Perform perimeter network reconnaissance/scanning.	Adversary uses commercial or free software to scan organizational perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks.
Perform network sniffing of exposed networks.	Adversary with access to exposed wired or wireless data channels used to transmit information, uses network sniffing to identify components, resources, and protections.
Gather information using open source discovery of organizational information.	Adversary mines publically accessible information to gather information about organizational information systems, business processes, users or personnel, or external relationships that the adversary can subsequently employ in support of an attack.
Perform reconnaissance and surveillance of targeted organizations.	Adversary uses various means (e.g., scanning, physical observation) over time to examine and assess organizations and ascertain points of vulnerability.
Perform malware-directed internal reconnaissance.	Adversary uses malware installed inside the organizational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.
Craft or create attack tools	
Craft phishing attacks.	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.
Craft spear phishing attacks.	Adversary employs phishing attacks targeted at high value targets (e.g., senior leaders/executives).

Craft attacks specifically based on deployed information technology environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organizational information technology environment.
Create counterfeit/spoof website.	Adversary creates duplicates of legitimate websites; when users visit a counterfeit site, the site can gather information or download malware.
Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.
Create and operate false front organizations to inject malicious components into the supply chain.	Adversary creates false front organizations with the appearance of legitimate suppliers in the critical life-cycle path that then inject corrupted/malicious information system components into the organizational supply chain.
Deliver/insert/install malicious capabilities	
Deliver known malware to internal organizational information systems (e.g., virus via email).	Adversary uses common delivery mechanisms (e.g., email) to install/insert known malware (e. g., malware whose existence is known) into organizational information systems.
Deliver modified malware to internal organizational information systems.	Adversary uses more sophisticated delivery mechanisms than email (e.g., web traffic, instant messaging, FTP) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems.
Deliver targeted malware for control of internal systems and exfiltration of data.	Adversary installs malware that is specifically designed to take control of internal organizational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions.
Deliver malware by providing removable media.	Adversary places removable media (e.g., flash drives) containing malware in locations external to organizational physical perimeters but where employees are likely to find the media (e.g., facilities parking lots, exhibits at conferences attended by employees) and use it on organizational information systems.
Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware or commercial information technology products. Adversary is not targeting specific organizations, simply looking for entry points into internal organizational information systems. Note that this is particularly a concern for mobile applications.
Insert targeted malware into organizational information systems and information system components.	Adversary inserts malware into organizational information systems and information system components (e.g., commercial information technology products), specifically targeted to the hardware, software, and firmware used by organizations (based on knowledge gained via reconnaissance).

Insert specialized malware into organizational information systems based on system configurations.	Adversary inserts specialized, non-detectable, malware into organizational information systems based on system configurations, specifically targeting critical information system components based on reconnaissance and placement within organizational information systems.
Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.
Insert tampered critical components into organizational systems.	Adversary replaces, though supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.
Install general-purpose sniffers on organization controlled information systems or networks.	Adversary installs sniffing software onto internal organizational information systems or networks.
Install persistent and targeted sniffers on organizational information systems and networks.	Adversary places within internal organizational information systems or networks software designed to (over a continuous period of time) collect (sniff) network traffic.
Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Adversary uses postal service or other commercial delivery services to deliver to organizational mailrooms a device that is able to scan wireless communications accessible from within the mailrooms and then wirelessly transmit information back to adversary.
Insert subverted individuals into organizations.	Adversary places individuals within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions.
Insert subverted individuals into privileged positions in organizations.	Adversary places individuals in privileged positions within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions. Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files, etc.) and may leverage access to one privileged capability to get to another capability.
Exploit and compromise	
Exploit physical access of authorized staff to gain access to organizational facilities.	Adversary follows (“tailgates”) authorized individuals into secure/controlled locations with the goal of gaining access to facilities, circumventing physical security checks.
Exploit poorly configured or unauthorized information systems exposed to the Internet.	Adversary gains access through the Internet to information systems that are not authorized for Internet connectivity or that do not meet organizational configuration requirements.
Exploit split tunneling.	Adversary takes advantage of external organizational or personal information systems (e.g., laptop computers at remote locations) that are simultaneously connected securely to organizational information

	systems or networks and to nonsecure remote connections.
Exploit multi-tenancy in a cloud environment.	Adversary, with processes running in an organizationally-used cloud environment, takes advantage of multi-tenancy to observe behavior of organizational processes, acquire organizational information, or interfere with the timely or correct functioning of organizational processes.
Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones).	Adversary takes advantage of fact that transportable information systems are outside physical protection of organizations and logical protection of corporate firewalls, and compromises the systems based on known vulnerabilities to gather information from those systems.
Exploit recently discovered vulnerabilities.	Adversary exploits recently discovered vulnerabilities in organizational information systems in an attempt to compromise the systems before mitigation measures are available or in place.
Exploit vulnerabilities on internal organizational information systems.	Adversary searches for known vulnerabilities in organizational internal information systems and exploits those vulnerabilities.
Exploit vulnerabilities using zero-day attacks.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Zero-day attacks are based on adversary insight into the information systems and applications used by organizations as well as adversary reconnaissance of organizations.
Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	Adversary launches attacks on organizations in a time and manner consistent with organizational needs to conduct mission/business operations.
Exploit insecure or incomplete data deletion in multitenant environment.	Adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment (e.g., in a cloud computing environment).
Violate isolation in multi-tenant environment.	Adversary circumvents or defeats isolation mechanisms in a multi-tenant environment (e.g., in a cloud computing environment) to observe, corrupt, or deny service to hosted services and information/data.
Compromise critical information systems via physical access.	Adversary obtains physical access to organizational information systems and makes modifications.
Compromise information systems or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organizations for purposes of subsequently infecting organizations when reconnected.
Compromise software of organizational critical information systems.	Adversary inserts malware or otherwise corrupts critical internal organizational information systems.

Compromise organizational information systems to facilitate exfiltration of data/information.	Adversary implants malware into internal organizational information systems, where the malware over time can identify and then exfiltrate valuable information.
Compromise mission-critical information.	Adversary compromises the integrity of mission-critical information, thus preventing or impeding ability of organizations to which information is supplied, from carrying out operations.
Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.
Conduct an attack (i.e., direct/coordinate attack tools or activities)	
Conduct communications interception attacks.	Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing publicly known flaws), targets those communications, and gains access to transmitted information and channels.
Conduct wireless jamming attacks.	Adversary takes measures to interfere with wireless communications so as to impede or prevent communications from reaching intended recipients.
Conduct attacks using unauthorized ports, protocols and services.	Adversary conducts attacks using ports, protocols, and services for ingress and egress that are not authorized for use by organizations.
Conduct attacks leveraging traffic/data movement allowed across perimeter.	Adversary makes use of permitted information flows (e.g., email communication, removable storage) to compromise internal information systems, which allows adversary to obtain and exfiltrate sensitive information through perimeters.
Conduct simple Denial of Service (DoS) attack.	Adversary attempts to make an Internet-accessible resource unavailable to intended users, or prevent the resource from functioning efficiently or at all, temporarily or indefinitely.
Conduct Distributed Denial of Service (DDoS) attacks.	Adversary uses multiple compromised information systems to attack a single target, thereby causing denial of service for users of the targeted information systems.
Conduct targeted DoS attacks.	Adversary targets DoS attacks to critical information systems, components, or supporting infrastructures, based on adversary knowledge of dependencies.
Conduct physical attacks on organizational facilities.	Adversary conducts a physical attack on organizational facilities (e.g., sets a fire).

Conduct physical attacks on infrastructures supporting organizational facilities.	Adversary conducts a physical attack on one or more infrastructures supporting organizational facilities (e.g., breaks a water main, cuts a power line).
Conduct cyber-physical attacks on organizational facilities.	Adversary conducts a cyber-physical attack on organizational facilities (e.g., remotely changes HVAC settings).
Conduct data scavenging attacks in a cloud environment.	Adversary obtains data used and then deleted by organizational processes running in a cloud environment.
Conduct brute force login attempts/password guessing attacks.	Adversary attempts to gain access to organizational information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.
Conduct non-targeted zero-day attacks.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Attacks are not based on any adversary insights into specific vulnerabilities of organizations.
Conduct externally-based session hijacking.	Adversary takes control of (hijacks) already established, legitimate information system sessions between organizations and external entities (e.g., users connecting from off-site locations).
Conduct internally-based session hijacking.	Adversary places an entity within organizations in order to gain access to organizational information systems or networks for the express purpose of taking control (hijacking) an already established, legitimate session either between organizations and external entities (e.g., users connecting from remote locations) or between two locations within internal networks.
Conduct externally-based network traffic modification (man in the middle) attacks.	Adversary, operating outside organizational systems, intercepts/eavesdrops on sessions between organizational and external systems. Adversary then relays messages between organizational and external systems, making them believe that they are talking directly to each other over a private connection, when in fact the entire communication is controlled by the adversary. Such attacks are of particular concern for organizational use of community, hybrid, and public clouds.
Conduct internally-based network traffic modification (man in the middle) attacks.	Adversary operating within the organizational infrastructure intercepts and corrupts data sessions.
Conduct outsider-based social engineering to obtain information.	Externally placed adversary takes actions (e.g., using email, phone) with the intent of persuading or otherwise tricking individuals within organizations into revealing critical/sensitive information (e.g., personally identifiable information).

Conduct insider-based social engineering to obtain information.	Internally placed adversary takes actions (e.g., using email, phone) so that individuals within organizations reveal critical/sensitive information (e.g., mission information).
Conduct attacks targeting and compromising personal devices of critical employees.	Adversary targets key organizational employees by placing malware on their personally owned information systems and devices (e.g., laptop/notebook computers, personal digital assistants, smart phones). The intent is to take advantage of any instances where employees use personal information systems or devices to handle critical/sensitive information.
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components.
Achieve results (i.e., cause adverse impacts, obtain information)	
Obtain sensitive information through network sniffing of external networks.	Adversary with access to exposed wired or wireless data channels that organizations (or organizational personnel) use to transmit information (e.g., kiosks, public wireless networks) intercepts communications.
Obtain sensitive information via exfiltration.	Adversary directs malware on organizational systems to locate and surreptitiously transmit sensitive information.
Cause degradation or denial of attacker-selected services or capabilities.	Adversary directs malware on organizational systems to impair the correct and timely support of organizational mission/business functions.
Cause deterioration/destruction of critical information system components and functions.	Adversary destroys or causes deterioration of critical information system components to impede or eliminate organizational ability to carry out missions or business functions. Detection of this action is not a concern.
Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement).	Adversary vandalizes, or otherwise makes unauthorized changes to, organizational websites or data on websites.
Cause integrity loss by polluting or corrupting critical data.	Adversary implants corrupted and incorrect data in critical data, resulting in suboptimal actions or loss of confidence in organizational data/services.
Cause integrity loss by injecting false but believable data into organizational information systems.	Adversary injects false but believable data into organizational information systems, resulting in suboptimal actions or loss of confidence in organizational data/services.
Cause disclosure of critical and/or sensitive information by authorized users.	Adversary induces (e.g., via social engineering) authorized users to inadvertently expose, disclose, or mishandle critical/sensitive information.

Cause unauthorized disclosure and/or unavailability by spilling sensitive information.	Adversary contaminates organizational information systems (including devices and networks) by causing them to handle information of a classification/sensitivity for which they have not been authorized. The information is exposed to individuals who are not authorized access to such information, and the information system, device, or network is unavailable while the spill is investigated and mitigated.
Obtain information by externally located interception of wireless network traffic.	Adversary intercepts organizational communications over wireless networks. Examples include targeting public wireless access or hotel networking connections, and drive-by subversion of home or organizational wireless routers.
Obtain unauthorized access.	Adversary with authorized access to organizational information systems, gains access to resources that exceeds authorization.
Obtain sensitive data/information from publicly accessible information systems.	Adversary scans or mines information on publicly accessible servers and web pages of organizations with the intent of finding sensitive information.
Obtain information by opportunistically stealing or scavenging information systems/components.	Adversary steals information systems or components (e. g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organizations, or scavenges discarded components.
Maintain a presence or set of capabilities	
Obfuscate adversary actions.	Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations.
Adapt cyberattacks based on detailed surveillance.	Adversary adapts behavior in response to surveillance and organizational security measures.
Coordinate a campaign	
Coordinate a campaign of multi-staged attacks (e.g., hopping).	Adversary moves the source of malicious commands or actions from one compromised information system to another, making analysis difficult.
Coordinate a campaign that combines internal and external attacks across multiple information systems and information technologies.	Adversary combines attacks that require both physical presence within organizational facilities and cyber methods to achieve success. Physical attack steps may be as simple as convincing maintenance personnel to leave doors or cabinets open.
Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome.	Adversary does not limit planning to the targeting of one organization. Adversary observes multiple organizations to acquire necessary information on targets of interest.
Coordinate a campaign that spreads attacks across organizational systems from existing presence.	Adversary uses existing presence within organizational systems to extend the adversary's span of control to other organizational systems including organizational infrastructure. Adversary thus is in position to further

	undermine organizational ability to carry out missions/business functions.
Coordinate a campaign of continuous, adaptive, and changing cyberattacks based on detailed surveillance.	Adversary attacks continually change in response to surveillance and organizational security measures.
Coordinate cyberattacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organizational operations.
Spill sensitive information	Authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
Mishandling of critical and/or sensitive information by authorized users	Authorized privileged user inadvertently exposes critical/sensitive information.
Incorrect privilege settings	Authorized privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low.
Communications contention	Degraded communications performance due to contention.
Unreadable display	Display unreadable due to aging equipment.
Earthquake at primary facility	Earthquake of organization-defined magnitude at primary facility makes facility inoperable.
Fire at primary facility	Fire (not due to adversarial activity) at primary facility makes facility inoperable.
Fire at backup facility	Fire (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Flood at primary facility	Flood (not due to adversarial activity) at primary facility makes facility inoperable.
Flood at backup facility	Flood (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Hurricane at primary facility	Hurricane of organization-defined strength at primary facility makes facility inoperable.
Hurricane at backup facility	Hurricane of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.

Resource depletion	Degraded processing performance due to resource depletion.
Introduction of vulnerabilities into software products	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.
Disk error	Corrupted storage due to a disk error.
Pervasive disk error	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.
Windstorm/tornado at primary facility	Windstorm/tornado of organization-defined strength at primary facility makes facility inoperable.
Windstorm/tornado at backup facility	Windstorm/tornado of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.

APPENDIX B: **Helpful Links**

CUSTOMIZABLE PRESENTATIONS FOR USE BY AIRPORT OPERATORS TO INTRODUCE THE IMPORTANCE AND APPLICABILITY OF CYBERSECURITY

- US-CERT's Protect Your Workplace Posters & Brochure: http://www.us-cert.gov/reading_room/distributable.html
- Socializing Securely: Using Social Networking Services: http://www.us-cert.gov/reading_room/safe_social_networking.pdf
- Governing for Enterprise Security: http://www.cert.org/governance/
- FFIEC Handbook Definition of Reputation Risk: http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-riskmanagement/reputation-risk.aspx
- What Businesses Can Do to Help with Cybersecurity: http://www.staysafeonline.org/sites/default/files/resource_documents/What%20Businesses%20Can%20Do%202011%20Final_0.pdf

TRAINING AND EXERCISES

- Free training materials, security configuration guides from Internet Security Alliance: http://www.isalliance.org/
- NIH Free Online User Training: http://iase.disa.mil/eta/issv4/index.htm
- NIH Free Online User Training (non DOD version): http://irtsectraining.nih.gov/publicUser.aspx
- International Information Systems Security Certification Consortium (ISC$^{2)}$: https://www.isc2.org/

OTHER CYBERSECURITY RESOURCES AND ORGANIZATIONS

- ASIS International Cybersecurity Center: https://www.asisonline.org/Membership/Member-Center/Security-Spotlight/Pages/Spotlight-on-CyberSecurity.aspx
- Airports Council International (ACI) – North America: https://aci-na.org/
- Aviation Information Sharing and Analysis Center (Aviation ISAC): https://www.a-isac.com/
- Information Systems Security Association (ISSA) - https://www.issa.org/
- ISACA - https://cybersecurity.isaca.org/csx-nexus
- International Organization for Standardization (ISO): https://www.iso.org/isoiec-27001-information-security.html
- SANS Institute: https://www.sans.org/
- Center for Internet Security (CIS): https://www.cisecurity.org/

FEDERAL AGENCY RESOURCES

- Department of Homeland Security
    - US Computer Emergency Readiness Team (US-CERT): https://www.us-cert.gov/
    - Transportation Security Administration: https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit

- National Institute of Standards and Technology (NIST): https://www.nist.gov/topics/cybersecurity
- NIST National Vulnerability Database: https://nvd.nist.gov/

LAW ENFORCEMENT AGENCIES

- U.S. Secret Service: https://www.secretservice.gov/investigation/#cyber
- Federal Bureau of Investigations: https://www.fbi.gov/investigate/cyber
- FBI Internet Crime Complaint Center: https://www.ic3.gov/default.aspx

CYBERSECURITY DOCUMENTS AND REPORTS

- Airport Cooperative Research Program (ACRP) Report 140 – *Guidebook on Best Practices for Airport Cybersecurity*: http://www.trb.org/Publications/Blurbs/172854.aspx
- 2017 IBM/Pokémon Data Breach Study - https://www.ibm.com/security/infographics/data-breach/
- 2017 Verizon Data Breach Study: https://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

APPENDIX C: **CEO Questions**

The following questions, while not entirely comprehensive, include many of the best practices for CEOs' understanding and awareness of their cybersecurity program. Below are questions that CEOs should be asking their executive, operational, and IT staff.

GOVERNANCE AND MANAGEMENT QUESTIONS

1. What regulations with cybersecurity aspects are we held to, and are we compliant (e.g., PCI-DSS, SSI, HIPAA, etc.)?
2. How is executive leadership informed about cyber risks?
3. Does our cybersecurity program apply any standards and best practices? What are they? How do we compare with other organizations of similar size and complexity?
4. How is risk measured? What is the level of impact of our cyber risks?
5. Do risk assessments address tenant and traveling public environment or impacts?
6. What is our plan to address the risks we have identified? What is the timeline and what resources are required?
7. Do our regular insurance policies cover cyber risk? Do we have a separate cybersecurity insurance policy? If so, what does it cover/not cover?
8. Does the cybersecurity program and risk review address both traditional IT systems (e.g., financial, HR, airport email, etc.) and our control systems (e.g., train, HVAC, airfield lighting, baggage, etc.)?
9. Do we know what data we share with third-party vendors or contractors? Do we know how these third parties safeguard our sensitive data when they have access to it? If they had a cybersecurity incident involving our data, would we know? Are they contractually obligated to safeguard our data and tell us if they have an incident?
10. Are board members or members of the airport's governing body going to be impacted if the airport has a cyber incident? For example, do board members use airport email systems to communicate or have access to special areas of the network to do their work?
11. Do our standard audits include cybersecurity issues? Has there been a cybersecurity audit or another type of formal assessment of risk, capabilities, and program maturity?
12. Is there an awareness of cybersecurity risks within the airport governing body? Do they frequently express interest/concern about the airport's cybersecurity or only when an incident somewhere else hits the news?
13. What kinds of cybersecurity training do we conduct? Do we train our users on our cybersecurity policies and expectations? Do we include training on emerging threats and new vulnerabilities that are being seen at other airports and elsewhere?
14. How frequently are our employees, contractors, and partners trained on our cybersecurity policies and expectations?

PROCESS QUESTIONS

15. How do we monitor our network for suspicious activity? How do we determine what suspicious activity looks like, and how do we decide what is important and what is not?
16. What is the threshold (severity, impact, etc.) for notifying executive leadership of these incidents? Who is responsible for making notification?
17. Is there a Cyber Incident Response Plan? How comprehensive is it? How often is it tested?
18. Who responds to cyber incidents? Who do we call for help if we need it? Who do we report incidents to?
19. Does our Cyber Incident Response Plan include communication and escalation protocols?
20. Do we participate in any programs to receive and share threat information with other airports? Are we part of any formal threat-information-sharing organizations?

TECHNOLOGY QUESTIONS

21. Do we regularly scan our network for vulnerabilities and have a program to fix any issues we uncover? Have we had an outside network penetration test performed recently? What were the results?
22. Is our wireless network encrypted? Do we offer secure connections to guests on our wireless networks so passengers and visitors can use their wireless devices without fear of someone intercepting their data?
23. If a new type of attack emerged, how long would it take for us to be able to detect it? How would we find out about it, and who is responsible for looking for new threats like this?
24. Are our network devices and personal computers running up-to-date software? Do we install patches to devices immediately when they are issued? If not, how do we prioritize and test software updates before installing them? How long does that take?
25. Do we encrypt our data when it is stored? Do we encrypt data that enters or leaves our network? Do our laptops, desktops, and mobile devices encrypt the data that is stored on them so that the data is protected if a device is lost or stolen?
26. Are the Industrial Control Systems (ICS) or SCADA devices running processes like our baggage, HVAC, electronic signage and other equipment or systems updated and patched? Who is responsible for this?
27. Do we know what airport processes and systems would be impacted in different types of events? Have outages or compromise of ICS equipment been included in these impact assessments?
28. How resilient are we (e.g., backups, redundancy, and speed to respond and recover)? Do we test recovery from cyberattacks as part of our regular IT business continuity testing?
29. Are our airport's ICS devices covered by our cybersecurity processes and tools? Would we be alerted if someone tried to take over our baggage handling system or HVAC system, for example?
30. How many and what types of cyber incidents are detected in a normal week? Are they increasing or decreasing over time? How many are successful?
31. How many of our monitoring, detection, and response activities are automated? How do we plan to keep up with increases in data as more parts of the airport are automated and connected to our network?
32. Are our key security tools automatically updated with new signatures and threats? If not, how long does it take for our threat detection to be brought up to date?

33. How quickly would we know if we were under attack, had a malware incident, or suffered a cyber intrusion? Have we tested those tools and procedures? Do we have any idea how long an attacker could go undetected in our network?
34. What networks are connected to ours? What tools are used to protect our network from a threat coming from a trusted partner's network? Have we tested those tools to make sure we are not vulnerable and would know if we were attacked from a partner network?

APPENDIX D: Interview Observations

As part of the project, the team met with and interviewed staff at a sample of airports to determine the state of the average airport's cybersecurity program, identify common issues and concerns, and identify areas where airports of specific sizes, governance models, or complexity might improve their cybersecurity readiness. The items below represent common themes that emerged from these interviews. Some of the themes might appear to be commonsense or established fact, but they all can have a real and consequential impact on airport cybersecurity.

- **Airport Industrial Control Systems (ICS) need attention.** Although many functions and services in the airport environment are controlled by Industrial Control Systems (ICS, also known as supervisory control and data acquisition [SCADA] systems), none of the airports we interviewed had given any thought to including security of network-addressable ICS systems as part of their cybersecurity program. The majority of airport IT teams indicated they had no insight into how the controllers for services such as baggage handling and HVAC were operated or were protected, even though most were addressable from the airport network. Some airport IT teams cited overt resistance by facilities engineering staff to sharing any information on ICS operations, and hostility towards discussing or implementing any security measures suggested by IT staff. *This appears to the project team to be an area ripe for urgent airport management intervention and leadership.*
- **Airports vary widely in the resources they devote to cybersecurity**. As would be expected, smaller and regional airports are severely limited regarding the financial and monetary resources they can devote to cybersecurity, while larger airports can often devote more resources.
- **Small airports are tempting targets.** Small to mid-sized airports, because of their lack of resources, are probably the most challenged by cybersecurity. Like small businesses in general, small community and regional airports often lack trained staff and the funds to purchase and operate cybersecurity tools. While they may not present as tempting a target as a large international airport, they will be targeted if for no other reason than they may be easy prey.
- **Few airports have dedicated cybersecurity resources.** While admittedly part of a small sample, only two of the airports stated they had a dedicated Chief Information Security Officer position. Most of the others relied on their IT services team to oversee cybersecurity activities for the airport, even though these teams may have little to no specific cybersecurity experience. Airports of all sizes may need to obtain outside help to gain the necessary specialty expertise in cybersecurity.
- **Airports that outsource cybersecurity tasks may lose oversight of incident reporting.** Cybersecurity is infrequently outsourced by any but the largest airports, but when it is, oversight and reporting of incidents may be lacking. Unless airport management requires that they be made specifically aware of incidents, they may only be told of the most severe incidents and have an inaccurate picture of the overall number and severity of cybersecurity incidents and near misses that involve their airport.
- **Cybersecurity rarely appears to be included in the overall airport security structure and often appears to be thought of as purely a technical or IT issue.** Cybersecurity response exercises may not be considered of equal importance to the traditional airport security exercise program. While airport physical security is highly structured and regulated, cybersecurity is less so and tends to be overlooked. This could easily lead to breakdowns in coordination between the physical and cybersecurity functions of an airport in a real-world incident.

- **Overall, few airports appear to regularly and systematically engage in cybersecurity incident response exercises.** While this project did not dig deeply into cybersecurity incident response planning at airports, many airports appear to have done some level of planning for incident response. Almost none, however, have included cyber incidents in their airport exercise programs.
- **Airport CEOs and Directors appear to vary widely in their personal involvement in their airport's cybersecurity program.** Some appear to be deeply involved and knowledgeable of their own roles and responsibilities in the program and the threats to their airports, while others are more hands-off in their approach to cybersecurity, believing their staff will handle cybersecurity concerns and tell them if there are issues. Unfortunately, this hands-off attitude is often interpreted as a lack of interest and support for an ongoing cybersecurity program. In addition, few airport IT staff appeared to have specifically trained and certified cybersecurity expertise on hand, which might easily cause a sub-par cybersecurity program to exist without management's knowledge.
- **Governance matters in airport cybersecurity**. Again, although based on a small sample, airports governed by an independent airport authority rather than as part of a city or county government appeared to have more flexibility in their cybersecurity programs, policies, finances, and planning. Airports governed by a city or county government appeared to have less ability to tailor their cybersecurity programs to rapidly changing threat environments, and appeared to operate under less flexible and adaptable cybersecurity policies and planning because they often must conform to centralized policies that do not take into account an airport's unique conditions and requirements.

APPENDIX E: Chief Information Security Officer (CISO) Duties and Responsibilities

- Act as the airport's primary senior executive point of contact for all matters relating to the security of the airport's IT networks, devices, and capabilities
- Ensure the security and privacy of airport customer, partner, and employee data
- Promote the airport's use of industry standards and best practices in cybersecurity and data privacy
- Direct and approve the design of information security systems, policies, and processes
- Review and approve security policies, controls, and cyber incident response planning
- Approve and oversee policies relating to the airport's user identity and access management policies
- Understand the IT threat landscape for the airport and airline industries, and identify security trends and evolving technologies
- Ensure continued compliance with laws and applicable regulations
- Schedule periodic security audits
- Conduct security awareness training to all personnel and enforce compliance
- Manage all teams, employees, and third parties involved in cyber security, which may include hiring
- Hire, train, and mentor security team members
- Conduct and supervise electronic discovery and digital forensic investigations
- Work with the legal counsel, privacy officer, and chief of airport security to achieve the organization's compliance with data privacy and security laws and regulations
- Brief the airport executive team on data risk management, including strategy and necessary budget
- Choose and purchase security products from vendors
- Identify and catalogue the types and sensitivity of data across the airport's network