ACRP

REPORT 140

AIRPORT
COOPERATIVE
RESEARCH
PROGRAM

Sponsored by
the Federal
Aviation
Administration

Guidebook on Best Practices for Airport Cybersecurity

TRANSPORTATION RESEARCH BOARD
OF THE NATIONAL ACADEMIES

ACRP OVERSIGHT COMMITTEE*

CHAIR

Kitty Freidheim
Freidheim Consulting

VICE CHAIR

Kelly Johnson
Northwest Arkansas Regional Airport Authority

MEMBERS

Deborah Ale Flint
Oakland International Airport
Thella F. Bowens
San Diego County Regional Airport Authority
Benito DeLeon
Federal Aviation Administration
Richard de Neufville
Massachusetts Institute of Technology
Kevin C. Dolliole
Unison Consulting
Steve Grossman
Jacksonville Aviation Authority
F. Paul Martinez
Dallas/Fort Worth International Airport
Bob Montgomery
Southwest Airlines
Eric Potts
Freese and Nichols, Inc.
Richard Tucker
Huntsville International Airport
Paul J. Wiedefeld
Baltimore/Washington International Airport

EX OFFICIO MEMBERS

Sabrina Johnson
U.S. Environmental Protection Agency
Richard Marchi
Airports Council International—North America
Laura McKee
Airlines for America
Melissa Sabatine
American Association of Airport Executives
T.J. Schulz
Airport Consultants Council
Neil J. Pedersen
Transportation Research Board
Gregory Principato
National Association of State Aviation Officials

SECRETARY

Christopher W. Jenks
Transportation Research Board

* Membership as of February 2015.

TRANSPORTATION RESEARCH BOARD 2015 EXECUTIVE COMMITTEE*

OFFICERS

CHAIR: **Daniel Sperling**, *Professor of Civil Engineering and Environmental Science and Policy; Director, Institute of Transportation Studies, University of California, Davis*
VICE CHAIR: **James M. Crites**, *Executive Vice President of Operations, Dallas/Fort Worth International Airport, TX*
EXECUTIVE DIRECTOR: **Neil J. Pedersen**, *Transportation Research Board*

MEMBERS

Victoria A. Arroyo, *Executive Director, Georgetown Climate Center; Assistant Dean, Centers and Institutes; and Professor and Director, Environmental Law Program, Georgetown University Law Center, Washington, DC*
Scott E. Bennett, *Director, Arkansas State Highway and Transportation Department, Little Rock*
Deborah H. Butler, *Executive Vice President, Planning, and CIO, Norfolk Southern Corporation, Norfolk, VA*
Jennifer Cohan, *Secretary, Delaware DOT, Dover*
Malcolm Dougherty, *Director, California Department of Transportation, Sacramento*
A. Stewart Fotheringham, *Professor, School of Geographical Sciences and Urban Planning, University of Arizona, Tempe*
John S. Halikowski, *Director, Arizona DOT, Phoenix*
Michael W. Hancock, *Secretary, Kentucky Transportation Cabinet, Frankfort*
Susan Hanson, *Distinguished University Professor Emerita, School of Geography, Clark University, Worcester, MA*
Steve Heminger, *Executive Director, Metropolitan Transportation Commission, Oakland, CA*
Chris T. Hendrickson, *Professor, Carnegie Mellon University, Pittsburgh, PA*
Jeffrey D. Holt, *Managing Director, Bank of Montreal Capital Markets, and Chairman, Utah Transportation Commission, Huntsville*
Geraldine Knatz, *Professor, Sol Price School of Public Policy, Viterbi School of Engineering, University of Southern California, Los Angeles*
Joan McDonald, *Commissioner, New York State DOT, Albany*
Abbas Mohaddes, *President and CEO, Iteris, Inc., Santa Ana, CA*
Donald A. Osterberg, *Senior Vice President, Safety and Security, Schneider National, Inc., Green Bay, WI*
Sandra Rosenbloom, *Professor, University of Texas, Austin*
Henry G. (Gerry) Schwartz, Jr., *Chairman (retired), Jacobs/Sverdrup Civil, Inc., St. Louis, MO*
Kumares C. Sinha, *Olson Distinguished Professor of Civil Engineering, Purdue University, West Lafayette, IN*
Kirk T. Steudle, *Director, Michigan DOT, Lansing*
Gary C. Thomas, *President and Executive Director, Dallas Area Rapid Transit, Dallas, TX*
Paul Trombino III, *Director, Iowa DOT, Ames*
Phillip A. Washington, *General Manager, Denver Regional Council of Governments, Denver, CO*

EX OFFICIO MEMBERS

Thomas P. Bostick (Lt. General, U.S. Army), *Chief of Engineers and Commanding General, U.S. Army Corps of Engineers, Washington, DC*
Timothy P. Butters, *Acting Administrator, Pipeline and Hazardous Materials Safety Administration, U.S. DOT*
Alison Jane Conway, *Assistant Professor, Department of Civil Engineering, City College of New York, NY, and Chair, TRB Young Members Council*
T. F. Scott Darling III, *Acting Administrator and Chief Counsel, Federal Motor Carrier Safety Administration, U.S. DOT*
Sarah Feinberg, *Acting Administrator, Federal Railroad Administration, U.S. DOT*
David J. Friedman, *Acting Administrator, National Highway Traffic Safety Administration, U.S. DOT*
LeRoy Gishi, *Chief, Division of Transportation, Bureau of Indian Affairs, U.S. Department of the Interior, Washington, DC*
John T. Gray II, *Senior Vice President, Policy and Economics, Association of American Railroads, Washington, DC*
Michael P. Huerta, *Administrator, Federal Aviation Administration, U.S. DOT*
Paul N. Jaenichen, Sr., *Administrator, Maritime Administration, U.S. DOT*
Therese W. McMillan, *Acting Administrator, Federal Transit Administration, U.S. DOT*
Michael P. Melaniphy, *President and CEO, American Public Transportation Association, Washington, DC*
Gregory G. Nadeau, *Acting Administrator, Federal Highway Administration, U.S. DOT*
Peter M. Rogoff, *Under Secretary for Transportation Policy, Office of the Secretary, U.S. DOT*
Mark R. Rosekind, *Administrator, National Highway Traffic Safety Administration, U.S. DOT*
Craig A. Rutland, *U.S. Air Force Pavement Engineer, Air Force Civil Engineer Center, Tyndall Air Force Base, FL*
Barry R. Wallerstein, *Executive Officer, South Coast Air Quality Management District, Diamond Bar, CA*
Gregory D. Winfree, *Assistant Secretary for Research and Technology, Office of the Secretary, U.S. DOT*
Frederick G. (Bud) Wright, *Executive Director, American Association of State Highway and Transportation Officials, Washington, DC*
Paul F. Zukunft (Adm., U.S. Coast Guard), *Commandant, U.S. Coast Guard, U.S. Department of Homeland Security*

* Membership as of May 2015.

AIRPORT COOPERATIVE RESEARCH PROGRAM

ACRP REPORT 140

Guidebook on Best Practices for Airport Cybersecurity

Randall J. Murphy
Michael Sukkarieh
GRAFTON TECHNOLOGIES, INC.
Newburyport, MA

Jon Haass
Paul Hriljac
SOFTKRYPT
Prescott, AZ

Subscriber Categories
Aviation • Data and Information Technology

Research sponsored by the Federal Aviation Administration

TRANSPORTATION RESEARCH BOARD

WASHINGTON, D.C.
2015
www.TRB.org

AIRPORT COOPERATIVE RESEARCH PROGRAM

Airports are vital national resources. They serve a key role in transportation of people and goods and in regional, national, and international commerce. They are where the nation's aviation system connects with other modes of transportation and where federal responsibility for managing and regulating air traffic operations intersects with the role of state and local governments that own and operate most airports. Research is necessary to solve common operating problems, to adapt appropriate new technologies from other industries, and to introduce innovations into the airport industry. The Airport Cooperative Research Program (ACRP) serves as one of the principal means by which the airport industry can develop innovative near-term solutions to meet demands placed on it.

The need for ACRP was identified in *TRB Special Report 272: Airport Research Needs: Cooperative Solutions* in 2003, based on a study sponsored by the Federal Aviation Administration (FAA). The ACRP carries out applied research on problems that are shared by airport operating agencies and are not being adequately addressed by existing federal research programs. It is modeled after the successful National Cooperative Highway Research Program and Transit Cooperative Research Program. The ACRP undertakes research and other technical activities in a variety of airport subject areas, including design, construction, maintenance, operations, safety, security, policy, planning, human resources, and administration. The ACRP provides a forum where airport operators can cooperatively address common operational problems.

The ACRP was authorized in December 2003 as part of the Vision 100-Century of Aviation Reauthorization Act. The primary participants in the ACRP are (1) an independent governing board, the ACRP Oversight Committee (AOC), appointed by the Secretary of the U.S. Department of Transportation with representation from airport operating agencies, other stakeholders, and relevant industry organizations such as the Airports Council International-North America (ACI-NA), the American Association of Airport Executives (AAAE), the National Association of State Aviation Officials (NASAO), Airlines for America (A4A), and the Airport Consultants Council (ACC) as vital links to the airport community; (2) the TRB as program manager and secretariat for the governing board; and (3) the FAA as program sponsor. In October 2005, the FAA executed a contract with the National Academies formally initiating the program.

The ACRP benefits from the cooperation and participation of airport professionals, air carriers, shippers, state and local government officials, equipment and service suppliers, other airport users, and research organizations. Each of these participants has different interests and responsibilities, and each is an integral part of this cooperative research effort.

Research problem statements for the ACRP are solicited periodically but may be submitted to the TRB by anyone at any time. It is the responsibility of the AOC to formulate the research program by identifying the highest priority projects and defining funding levels and expected products.

Once selected, each ACRP project is assigned to an expert panel, appointed by the TRB. Panels include experienced practitioners and research specialists; heavy emphasis is placed on including airport professionals, the intended users of the research products. The panels prepare project statements (requests for proposals), select contractors, and provide technical guidance and counsel throughout the life of the project. The process for developing research problem statements and selecting research agencies has been used by TRB in managing cooperative research programs since 1962. As in other TRB activities, ACRP project panels serve voluntarily without compensation.

Primary emphasis is placed on disseminating ACRP results to the intended end-users of the research: airport operating agencies, service providers, and suppliers. The ACRP produces a series of research reports for use by airport operators, local agencies, the FAA, and other interested parties, and industry associations may arrange for workshops, training aids, field visits, and other activities to ensure that results are implemented by airport-industry practitioners.

ACRP REPORT 140

Project 05-02
ISSN 1935-9802
ISBN 978-0-309-30880-9
Library of Congress Control Number 2015942910

© 2015 National Academy of Sciences. All rights reserved.

COPYRIGHT INFORMATION

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

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

NOTICE

The project that is the subject of this report was a part of the Airport Cooperative Research Program, conducted by the Transportation Research Board with the approval of the Governing Board of the National Research Council.

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 the Transportation Research Board and approved by the Governing Board of the National Research Council.

The opinions and conclusions expressed or implied in this report are those of the researchers who performed the research and are not necessarily those of the Transportation Research Board, the National Research Council, or the program sponsors.

The Transportation Research Board of the National Academies, the National Research Council, and the sponsors of the Airport Cooperative Research Program do not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the object of the report.

Published reports of the

AIRPORT COOPERATIVE RESEARCH PROGRAM

are available from:

Transportation Research Board
Business Office
500 Fifth Street, NW
Washington, DC 20001

and can be ordered through the Internet at

http://www.national-academies.org/trb/bookstore

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. C. D. Mote, Jr., is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Victor J. Dzau is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. C. D. Mote, Jr., are chair and vice chair, respectively, of the National Research Council.

The **Transportation Research Board** is one of six major divisions of the National Research Council. The mission of the Transportation Research Board is to provide leadership in transportation innovation and progress through research and information exchange, conducted within a setting that is objective, interdisciplinary, and multimodal. The Board's varied activities annually engage about 7,000 engineers, scientists, and other transportation researchers and practitioners from the public and private sectors and academia, all of whom contribute their expertise in the public interest. The program is supported by state transportation departments, federal agencies including the component administrations of the U.S. Department of Transportation, and other organizations and individuals interested in the development of transportation. **www.TRB.org**

www.national-academies.org

COOPERATIVE RESEARCH PROGRAMS

CRP STAFF FOR ACRP REPORT 140

Christopher W. Jenks, *Director, Cooperative Research Programs*
Michael R. Salamone, *ACRP Manager*
Marci A. Greenberger, *Senior Program Officer*
Joseph J. Snell, *Senior Program Assistant*
Eileen P. Delaney, *Director of Publications*
Natalie Barnes, *Senior Editor*

ACRP PROJECT 05-02 PANEL
Field of Security

Royce Holden, *Greater Asheville Regional Airport Authority, Fletcher, NC* (Chair)
Caroline Barnes, *FBI Newark Division, Newark, NJ*
John McCarthy, *Service Tec International, Reston, VA*
David E. Wilson, *Port of Seattle, Seattle-Tacoma International Airport, Seattle, WA*
Martha A. Woolson, *Alexandria, VA*
Abel Tapia, *FAA Liaison*
Aneil Patel, *Airports Council International–North America Liaison*
Christine Gerencher, *TRB Liaison*

AUTHOR ACKNOWLEDGMENTS

The research reported herein was performed under ACRP Project 05-02 by Grafton Technologies, Inc.; SoftKrypt; and Grafton Information Services, Inc. with airport advisory services provided by the Massachusetts Port Authority (Massport). Randall J. Murphy, President of Grafton Technologies, Inc. was the Principal Investigator. The other authors of this report are Dr. Jon Haass, Associate Professor of Cyber Intelligence and Security at Embry-Riddle Aeronautical University (ERAU) and Chief Executive Officer at SoftKrypt; Dr. Paul Hriljac, Professor of Mathematics and Computer Science at ERAU and Chief Technical Officer at SoftKrypt; Michael Sukkarieh, cybersecurity expert at Grafton Technologies, Inc.; Thomas Crossman, Project Researcher at Grafton Technologies, Inc.; Patrick McHallam, Application Developer at Grafton Technologies, Inc.; and Maureen Murphy, Project Administrator at Grafton Information Services, Inc. Tom Domenico, Director of Cyber Security & Public Safety Systems at Massport, and Jeffrey W. Jordan, Senior Project Manager of the Information Technology Department at Massport, provided airport advisory services to the project team.

FOREWORD

By Marci A. Greenberger
Staff Officer
Transportation Research Board

ACRP Report 140: Guidebook on Best Practices for Airport Cybersecurity provides resources for airport managers and information technology (IT) staff to reduce or mitigate inherent risks of cyberattacks on technology-based systems. Traditional IT infrastructure such as servers, desktops, and network devices are covered along with increasingly sophisticated and interconnected industrial control systems, such as baggage handling, temperature control, and airfield lighting systems. Accompanying this guidebook is a CD-ROM of multimedia material that can be used to educate all staff at airports about the need, and how, to be diligent against cybersecurity threats.

Cybersecurity is a growing issue for all organizations, including airports. While the risks to traditional IT infrastructure are often highlighted, many airports also rely on industrial control systems that introduce risks that are less apparent. The increasing practice of Bring Your Own Device (BYOD), whereby employees use their own personal devices for business purposes such as email and remote access to airport systems, brings its own risks that must be managed. These risks cannot be eliminated, but they can be reduced through implementation of industry standards, best practices, and awareness programs for employees.

Grafton Technologies, Inc., as part of ACRP Project 05-02, conducted research on risks and practices from within and outside of airports to develop these best practices and resources. The multimedia material that can be found in the CD-ROM can help make employees and consultants aware of the various ways in which cyberattacks can occur and what they can do to mitigate and prevent them from being successful.

Airport chief information officers, IT managers, and all airport staff, as well as consultants, tenants, and others who conduct business at airports, will find information and resources that will be useful and applicable to their responsibilities at the airport.

CONTENTS

1 Summary

4 **Chapter 1** Introduction

7 **Chapter 2** What Is Cybersecurity?

10 **Chapter 3** An Approach to Cybersecurity at Airports

10 Overview
10 Primary Activities
12 Key Roles and Responsibilities
12 Cybersecurity Tasks
14 Threats
15 Affected Data and Systems
18 Countermeasures

20 **Chapter 4** Implementing Countermeasures

20 Airport Systems
20 IT Infrastructure
22 End-Point Systems
23 Industrial Control Systems
26 Wi-Fi
27 Cloud-Based Services
28 Global Positioning System
28 Human Considerations
29 Social Engineering
30 Bring Your Own Device
32 Use of Social Media
33 Malicious Insiders
34 Service Providers
34 Service Providers That Can Increase the Likelihood of a Cyberattack
35 Service Providers That Help Protect an Airport
37 Passengers, Greeters, and Other Occupants
38 Private, Confidential, and Sensitive Information

39 **Chapter 5** Developing a Cybersecurity Program

39 Cybersecurity Governance
40 Legal Requirements and Regulation
41 Standards and Guidelines
43 Payment Card Industry Data Security Standards
46 Policies
47 Contracts and Procurement Considerations
49 Software and Information Security Assurance

51 Resources Required
52 Staffing
56 Funding
58 External Support
59 Cybersecurity Training
60 Awareness Training
61 Specialized Training
62 Training Resources
62 Sustaining a Cybersecurity Program
63 Risk of Implementing a Cybersecurity Program

65 Chapter 6 Detecting, Responding to, and Recovering from Attacks
65 Detecting Attacks
67 Responding to an Attack
68 Recovery to Normal Operations
69 Lessons Learned

70 Chapter 7 Conclusions and Suggested Research
70 Conclusions
71 Suggested Research

73 Glossary, Abbreviations, Acronyms, and Symbols

76 References

80 Appendix A Categorized List of Cybersecurity Threats

89 Appendix B Airport Systems

94 Appendix C Countermeasures

149 Appendix D Using the Multimedia Material

Note: Photographs, figures, and tables in this report may have been converted from color to grayscale for printing. The electronic version of the report (posted on the web at www.trb.org) retains the color versions.

SUMMARY

Guidebook on Best Practices for Airport Cybersecurity

Cyber, or computer-based, threats are growing in number and sophistication. Although this trend is well publicized in the media, it is not as apparent that airports have been targeted and that some have fallen victim to cyberattack. The result has been the loss of confidential data, disruption to operations, costly recoveries, and degraded reputation. Such attacks are likely to become more common as airports increasingly rely on computing technology and cyberattackers become more sophisticated.

The technology that may be affected is not limited to the desktop computers, servers, and network devices that compose typical information technology (IT) infrastructure. Flight information display systems (FIDS), airfield lighting controls, heating and ventilation systems, baggage handling systems, access control devices, and a broad range of other mission-critical systems rely on digital technology that may be vulnerable to attack. Since these systems are often not regarded as computing devices, cybersecurity protective measures are often not applied.

Attacks against systems not owned by an airport can also have an impact and should be protected to the extent feasible through contracts and agreements. Airlines, concessionaires, and other tenants may utilize airport data, systems, and network resources in a manner that can introduce vulnerabilities. This interconnectivity is increasing as airports and their stakeholders leverage digital technology to work together more efficiently. Some airports also allow employees to use their own smartphones, tablets, and computers for work purposes. There are many advantages of this approach, but it can also introduce many new vulnerabilities that must be addressed. Another trend is that airports are increasingly relying on computing services delivered via the Internet, an approach referred to as cloud-based computing. When using the cloud, airports no longer have the same level of control over the security of their data and systems, so additional precautions are warranted, and reputable providers must be selected.

Despite the advanced technologies and sophisticated approaches used by attackers, some of the most basic vulnerabilities are where attacks begin. Many of these vulnerabilities are related to human activity. Poor handling of usernames and passwords, clicking on links from disguised sources, downloading suspicious software, and exposing sensitive information have led to many successful attacks. Often, advanced attackers will leverage one success to launch subsequent, more invasive attacks that target sensitive data and systems.

To protect themselves, airport managers, IT professionals, staff, tenants, and consultants need to be aware that these threats exist, of the impact these threats may have on critical data and systems, and of the measures they can take to protect the airport. Their goal should be to implement countermeasures that satisfy the risk aversion of those responsible for airport safety and efficiency to the extent available staff and funding allow. Perfect protection is not attainable, nor perhaps advisable, due to the expense. Multiple layers of defense that address the highest priority vulnerabilities, or "defense in depth," should be the goal.

This guidebook and the associated multimedia material on the accompanying CD-ROM offer airports an approach to attain this goal. The guidelines provided are based on the best practices of the airport industry and also other industries, such as financial services, electrical transmission, and health care that have had to deal with these challenging problems for many years. Resources are provided to increase awareness and to train staff and other key stakeholders.

Findings

Most airports are taking steps to protect themselves from cyber threats. Virus protection software, network firewalls, and network password controls are common. Many airports have formalized their approach by establishing a cybersecurity program, often writing down the policies and procedures that program entails. A growing number of airports have appointed a chief information security officer (CISO) to lead these efforts. A few employ highly qualified technical staff to implement state-of-the-art protection.

Cybersecurity best practices are, however, not being universally applied by airports. The importance of cybersecurity is often not emphasized outside of an airport's IT department; senior managers often do not fully appreciate the importance of cybersecurity when making funding decisions; and staff are often untrained, resulting in poor habits that expose vulnerabilities. There are a growing number of resources, many freely available, that are not being fully tapped by airports. These include support from federal agencies, relevant information sharing forums, cybersecurity training programs, and relevant literature.

Based on the research that was conducted for this project, the following are some of the cybersecurity best practices that airports should consider:

- 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.
- Establish and enforce policies for acceptable use, sensitive security information (SSI), information privacy, software and data assurance, training, and communications.
- 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.
- Maintain an inventory of data, systems, network devices, and users that may be affected by a cyberattack.
- Identify vulnerabilities where these assets are not adequately protected and prioritize them based on the impact a successful attack may have.
- Implement countermeasures to achieve the level of protection that is desired and affordable.
- Assign CISO responsibilities to a qualified staff member, new hire, or consultant.
- Monitor computer and human behavior through manual and automated means.
- Communicate anomalous activity and successful attacks to the CISO, IT staff, senior management, affected stakeholders, other agencies, and law enforcement personnel.
- Be prepared to isolate affected systems, remove them, recover from attacks, and learn from them.
- Recognize that, even if all of 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.

No airport is too small or too large to take these measures. There is no minimum threshold of investment that is required. The challenge is to balance the degree of risk that is acceptable with the opportunity cost of dedicating resources to other activities. Achieving this balance requires senior managers who are responsible for managing risk to work with IT and facility managers

who are responsible for the data and systems that can create the risk. Technical advisors may also be required to summarize the salient details.

Conclusions

Cybersecurity has become a cost of doing business for airports. All airports can afford it; it is a matter of how much and what sacrifices they are willing to make. Regardless of the level they choose, all airports make this determination either proactively or by default. As cybersecurity awareness increases, more airports are choosing to be proactive. They are appointing CISOs, establishing policies and procedures, training staff, implementing technical countermeasures, preparing their response should an attack occur, and sharing their results with peers. This trend is likely to continue and, as it does, that gap between the capabilities of the offense (i.e., attackers) and the defense (i.e., airport managers and staff) will shrink.

Recommendations

This guidebook and the associated multimedia material provide one of many resources to help airports achieve the goal of establishing a cybersecurity program that is founded on best practice. It is recommended that airport managers use these resources to help them establish a comprehensive cybersecurity program. Those that already have a cybersecurity program can use this guidebook to confirm that they have implemented best practices or to provide ideas on further improvements they can make. After establishment of a program that meets current industry best practices, airports are advised to continue to be vigilant and to use all resources, including those in this guidebook, to adapt to the constantly evolving threat of cyberattacks.

CHAPTER 1

Introduction

Airport managers and staff; airline, concession, and other tenants; contractors and consultants; travelers; and shippers are progressively reliant on computers, electronic devices, and network infrastructure. These rapidly advancing technologies offer better service, enhanced capacity, improved safety, and operational efficiency. Unfortunately, they also increase an airport's exposure to individuals, organizations, and countries looking to cause disruption, steal information, or harm critical infrastructure by exploiting weaknesses in technology. They also create opportunities for insiders to deliberately cause harm or well-intentioned individuals to make mistakes that can have similar consequences. An increased use of technology within an environment of increasing threat necessitates a vigilant approach to cybersecurity.

An increased use of technology within an environment of increasing threat necessitates a vigilant approach to cybersecurity.

The objective of this guidebook is to provide guidance that will help airports achieve that vigilance by implementing cybersecurity best practices. It offers an approach to identifying threats, prioritizing them based on the potential impact they may have on critical systems, and implementing countermeasures that can help airports prevent and recover from successful attacks.

These guidelines will help airports establish an effective cybersecurity program that fits their budget and technical capabilities. They can also help airports that already have an established cybersecurity program validate or improve their program based on industry best practices. The best practices are based on lessons learned from peer airports as well as organizations in financial, health care, utility transmission, communications, and defense industries. This guidebook also identifies government resources, guidelines, policies, and regulations that have been rapidly emerging to help thwart the growing threat of cyberattack within the United States. Private-sector resources are described along with suggestions on how to identify and select the most appropriate product or resource.

This report provides guidance on establishing and maintaining a cybersecurity program based on industry best practices.

After this introduction, Chapter 2 of this guidebook defines cybersecurity and highlights why it is a subject of growing importance. Chapter 3 offers an approach to addressing the cybersecurity needs of an airport, detailing the threats that exist, the airport systems that may be vulnerable, and the countermeasures that can be taken to reduce those vulnerabilities or to respond if an attack is successful. These and other basic terms are shown conceptually in Figure 1. Chapter 4 provides specific details on implementing countermeasures in key areas of vulnerability. Each area is introduced; common threats are identified; countermeasures are recommended; and additional resources are offered. Chapter 5 provides guidance on establishing and maintaining a cybersecurity program based on industry best practices. Throughout the guidebook symbols are used to denote threats (), affected data and systems (), countermeasures (), and resources ().

This guidance is intended to help those responsible for cybersecurity at an airport prioritize, fund, and execute the most relevant aspects of a strong program. Finally, the guidebook identifies ongoing activities that airports should follow to detect and respond to attacks. Appendixes

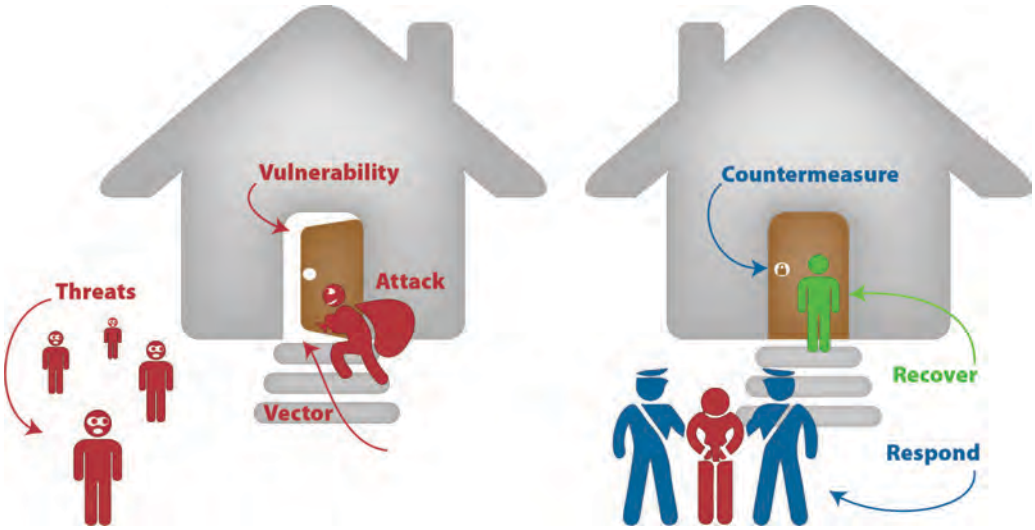


Figure 1. Basic cybersecurity terms.

provide a glossary of relevant terms. Throughout the guidebook are references to literature and public resources that airport managers and staff may find helpful.

Research findings from this project indicate that chief information officers (CIOs), IT managers, CISOs, cybersecurity managers, other staff positions, and a few chief executive officers (CEOs) [based on 41 of 44 (93%) of those that responded to the question] are the ones responsible for establishing and maintaining airport cybersecurity programs. This guidebook is intended to help them fulfill this responsibility by offering guidance, resources, and tools.

This guidebook is accompanied by a CD containing multimedia material that offers airports training, documentation, tools, and resources that they can leverage to cost-effectively implement cybersecurity best practices. The audience for this multimedia material encompasses airport senior management, IT managers, department managers, and staff. Other airport stakeholders such as agencies that oversee airports, airlines, concessionaires, consultants, contractors, and others may find the material helpful as well. Both this written guidebook and the accompanying multimedia material are organized to make it easy for readers to find the material best suited for them. This multimedia material should work on any computer and does not require technical expertise to use.

Content that is supported by relevant multimedia material is highlighted with an icon (shown at left) and enclosed in a box. Instructions on how to use the multimedia material can be found in Appendix D.

This guidebook and the accompanying multimedia material were developed based on targeted industry research as well as on the experience of the research team and its advisors. The research started with a literature search to identify relevant (and credible) research papers, journal articles, conference proceedings, research papers, and books on airport cybersecurity and related topics. These documents were reviewed and relevant findings were extracted and included in the report, as cited. In addition, dialogue with the growing number of researchers, committee chairs, and association members who are focused on cybersecurity helped identify the current state of practice. Next, airports and other relevant organizations were asked to complete an online survey,

the results of which are incorporated into these materials. Although care must be taken when interpreting the results of any small population survey, the findings and trends identified are supportive. The survey led to face-to-face and telephone interviews with personnel at airports that have exemplary cybersecurity programs as well as industry, government, and private-sector providers who supplied complementary information and resources.

The project deliverables also benefitted from the years of experience and background of the research team. The research team included individuals each with decades of experience in airport IT or cybersecurity. It was augmented by a team member with many years of experience in implementing cybersecurity best practices within the financial sector. Team advisors from a major airport's IT department helped ensure the results are applicable within typical airport organizations.

The research that was conducted was also guided by a panel of experts assembled by the Airport Cooperative Research Program (ACRP). This panel included airport IT managers, representatives from federal agencies, an airport industry association, and consultants focused on cybersecurity. Their guidance during the proposal development, work planning, interim, and final deliverable stages of this project ensured that the guidebook addresses airport industry cybersecurity needs.

Although the collective efforts of the research team, advisors, and panel members have contributed to the applicability, the thoroughness, and the quality of this guidebook, there are some inherent limitations:

- The realm of cybersecurity is rapidly changing. This guidebook was written to have as much longevity as possible but to provide specifics; it is likely that some findings will soon be out of date.
- Much of the information provided was shared on the condition of anonymity because of its sensitive, proprietary, or confidential nature. The result is that many of the findings are generalized indicating the proportion, trend, or type of respondent and not providing details that respondents asked not be shared.
- Care was taken to ensure that the information provided in this guidebook can be used to help airports protect themselves against cyberattack but that it did not provide details that would help potential attackers. This concern is shared by authors of similar documents in the industry. Some industry experts, however, suggest that modern cybercriminals are very sophisticated and not likely informed by guidance such as found in these deliverables. It was further noted that many of the protective measures that can have a significant impact are commonly known, just not commonly implemented.
- There are many private-sector products and resources that can help airports establish and maintain cybersecurity programs. Recommendations of individual companies or consultants, however, are not provided in this guidebook or the accompanying multimedia material.

To help address these limitations, the following forums are recommended and may provide the longevity, specifics, and referrals that this guidebook cannot. They are provided as a means of augmenting the resources cited in the remainder of the guidebook.

- Airports Council International–North America's Business Information Technology Committee: www.aci-na.org/committee/business-information-technology/
- Aviation Information Sharing and Analysis Center: a-isac.com/
- Multi-State Information Sharing and Analysis Center: msisac.cisecurity.org/
- National Crime Information Center: fas.org/irp/agency/doj/fbi/is/ncic.htm/
- National Institute of Standards and Technology: www.nist.gov
- TRB's Cybersecurity Subcommittee (sponsored under ABE40): www.abj50.org/subcommittees/cybersecurity/

CHAPTER 2

What Is Cybersecurity?

"Cyber" encompasses the computers, servers, and network components that form traditional IT infrastructure. It also includes the software used and the information transmitted over this infrastructure. Industrial control systems (ICS)—such as airfield lighting; heating, ventilation, and air conditioning (HVAC); and baggage handling systems—are also part of an airport's cyber infrastructure. Together these systems support the safe operation of aircraft, development and maintenance of airport facilities, check-in and screening of passengers, and a variety of other activities.

The breadth of cyber systems found at an airport is growing as new systems and technologies become available not only to airport management and staff, but also to the airlines, tenants, and ultimately the passengers they serve. Rapidly advancing mobile computing capabilities are also encouraging some airports to rely on public cellular or wireless networks to extend the reach of their cyber systems within terminals and onto airfields. Some airports have a Bring Your Own Device (BYOD) policy, which allows their employees to use personal phones and tablets to perform work duties. The breadth of an airport's cyber systems is also not bounded by its network or facilities. An increasing number of airports are relying on computer infrastructure, software, and data on the Internet or in the "cloud."

Cybersystems are a key and growing component of an airport's infrastructure.

As the number and breadth of cyber systems in use at airports grow, so does the risk of cyberattack. The expanded use of commonly used technologies, the increasing exchange of information between systems, and the criticality of their use increase the likelihood and potential impact of these attacks.

Like any element of an airport's critical infrastructure, systems and their data must be protected. Threats may be intentional, coming from sophisticated actors in well-funded countries or organizations, disgruntled staff or customers who already have access, or individual pranksters. Threats may also be unintentional such as a mistaken release of sensitive information. Some respondents to this project's online survey assumed that "if it's not connected to the Internet, it's not vulnerable to cyberattack." Unfortunately, this assertion has been proven wrong by many successful attacks that were not via the Internet. As one interview respondent said, "If bits or bytes pass through it, it may be vulnerable."

"If bits or bytes pass through it, it may be vulnerable."
–Survey respondent

While the percentage of cyber threats that are averted remains very high, the number of threats has grown significantly and the damage caused by the threats that do get through is greater (Gilliland 2014). This is one of the reasons that the majority of respondents (22 of 40 or 55%) feels that the degree of cyber risk their organizations face has increased over the last year. Their concerns are warranted, as the following list of successful cyberattacks on airports suggests:

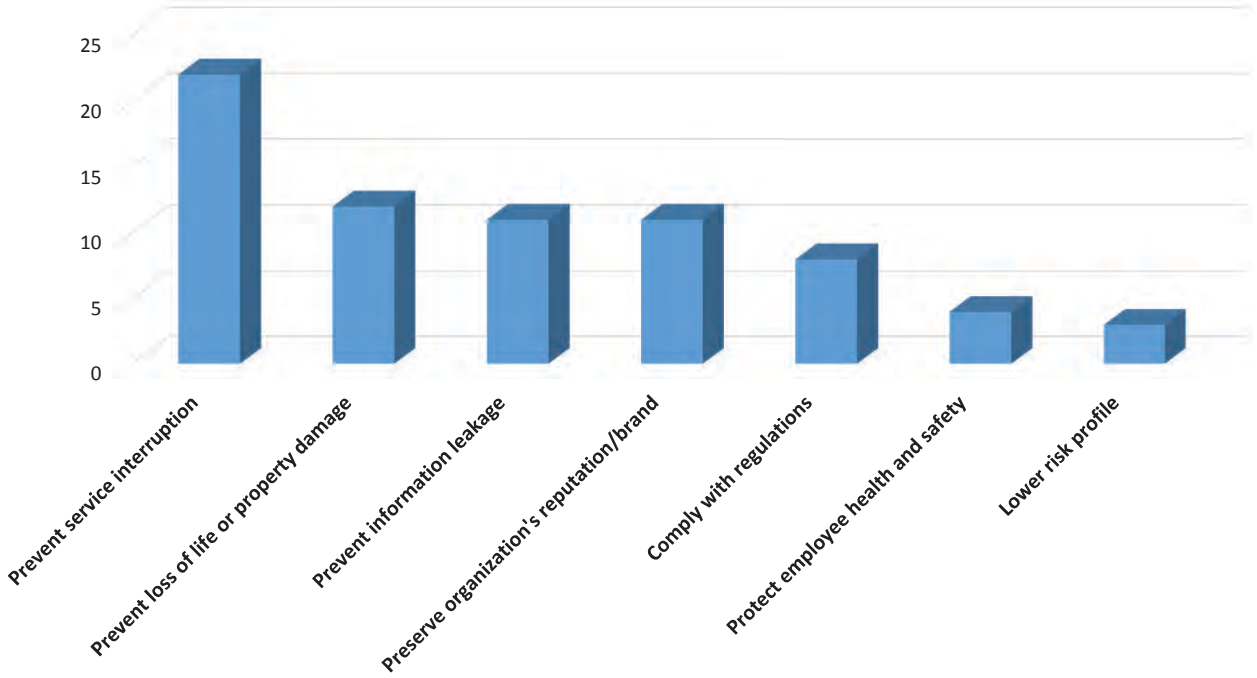
- A sophisticated advanced persistent threat from a sophisticated group of hackers acting on behalf of a nation state used a reputable industry source to send phishing emails to airports.

Seventy-five airports were affected and two had systems that were compromised as a result (Center for Internet Security 2013).

- The Airport Operations Division of the Metropolitan Washington Airport Authority unintentionally published a request for procurement (RFP) on its website containing sensitive security information (SSI) detailing the outsourced electronic security system at the Ronald Reagan Washington National Airport (DCA). This RFP was not vetted through the IT department.
- Miami International Airport (MIA) has experienced almost 20,000 hack attempts per day before investing in training, education, and new hardware to protect itself from cyberattacks (Palmer 2013).
- Los Angeles World Airports (LAX, ONT, VNY, and PMD) blocked almost 60,000 cases of Internet misuse and 2.9 million hacking attempts in one year. LAX also experienced a number of cyber incidents related to malware that targeted a network baggage system (Cheong 2011).
- U.S. airport computer and communications systems were among the targets announced by the Tunisian Hackers Team in April 2014 (Kimery 2014).
- Researchers have demonstrated that some passenger screening devices used by the Transportation Security Administration (TSA) can be tampered with so that they do not provide the proper alerts if an attacker gains physical access to data ports on the devices (Rios 2014). Although not directly the responsibility of the airport, compromised TSA equipment could impair airport operations and expose additional vulnerabilities.
- A truck driver jamming his vehicle's global positioning system (GPS) receiver inadvertently interfered with an airport GPS augmentation system used to support aircraft approach procedures at Newark International Airport (EWR).
- Istanbul's Atatürk International Airport (IST) had password control systems shut down by what is believed to have been a malware attack resulting in departure delays and extended waiting time for passengers (Paganini 2013).
- An undisclosed major, non-U.S., international airport uncovered a variant of the Citadel Trojan malware that targeted virtual private network (VPN) credentials used by employees (Klein 2012, Kumar 2012).
- The Dubai International Airport (DXB) had 50 email addresses and associated passwords stolen by a team of hackers from the Portugal Cyber Army and the HighTech Brazil HackTeam (Selvan 2013).
- The website of Catania–Fontanarossa Airport (CTA) in Italy was hacked and shut down for a few hours. A 22-year-old suspect was believed to have illegally accessed and damaged data (Kumar 2011).
- The Airports Authority of India's enterprise resource planning system was successfully hacked resulting in the system becoming inoperative, but more importantly resulting in the loss of personal data on employees (Vijay 2014, The Asian Age 2014).

To combat these and other potential cyberattacks, many airports have taken measures to protect their data and systems. As Figure 2 shows, the top rationale for taking such measures is to prevent service interruptions, although preventing property damage or loss of life, preventing loss of information, preserving the airport's reputation, and complying with regulations are key motivators as well.

Driven by these motivators, many airports have established cybersecurity programs [according to 32 of 41 (78%) survey respondents who answered this question]. Most of these programs are based on written organizational policy [24 of 32 respondents (75%) of those who answered this question]. These programs often encompass an inventory of critical systems and assets, vulnerability assessments, monitoring for anomalous activity, configuration management, physical security, training, and other measures. Unfortunately, only about half of survey respondents who answered this question [19 of 39 (49%)] felt that these measures provided adequate protection.



Source: 27 of 55 (49%) survey respondents.

Figure 2. Reasons for implementing cybersecurity.

Fortunately, there is a growing number of resources that an airport can use to protect its data and systems. This mitigation requires specialized technical skills, software, and hardware as well as well-defined policies and procedures. While some airports have been able to provide such protection, not all airports can obtain, retain, and maintain the necessary staff and infrastructure. There is, however, a growing number of public and private organizations that can help airports establish and maintain effective cybersecurity programs. The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, the Department of Homeland Security (DHS)–funded Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Payment Card Industry (PCI) Data Security Standards (DSS) are just a few of the resources airports have tapped. The remainder of this guidebook is intended to help airports develop, and then to maintain, an approach to cybersecurity that leverages these organizations and other resources.

CHAPTER 3

An Approach to Cybersecurity at Airports

The underlying goal should be to identify and address vulnerabilities to satisfy the risk tolerance of senior management in an efficient and cost-effective manner.

Overview

The core of a cybersecurity program is the approach that is used to identify, assess, and reduce the risk of successful attack. This process can be implemented in phases but must remain flexible to respond to new risks as they arise. The goal is to implement multiple layers of countermeasures that are deployed throughout an airport's systems, data, infrastructure, and personnel. This is referred to as "defense in depth." The essential elements of such an approach are illustrated in Figure 3 and detailed in subsequent sections of this guidebook. This process should be led and managed by the CISO or a similar position that senior management has entrusted to manage the airport's risk of being impacted by cyberattack.

The process described in Figure 3 is included in the multimedia material for IT staff.

Primary Activities

The steps illustrated in Figure 3 are organized into columns representing primary activities established by the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST 2014). The primary activities defined by the NIST Framework are listed below and illustrated as columns in Figure 3:

1. **Identify** the equipment, software, business practices, and data flows within the organization, its networks and subnetworks. This inventory is required in order to understand the scope of implementing comprehensive protective measures but also to organize the myriad of details that are necessary, especially in the event of an attack. This inventory process needs to be an ongoing activity because systems frequently change, software is updated, and new personnel are hired.
2. **Protect** systems, data, and infrastructure by implementing and updating countermeasures in a prioritized manner through monitoring.
3. **Detect** cyberattacks in a timely manner by monitoring for anomalous activity on end-point systems, IT and communications networks, and in areas where sensitive IT and ICS infrastructure exists. It is important to periodically test the detection mechanisms for proper configuration and response to reduce both false positives and missed negatives.
4. **Respond** to cybersecurity attacks in a quick and effective manner, while minimizing the duration and extent of their impact. Effective response begins before an attack occurs with planning on how to react and with the collection of information and contacts that can help.

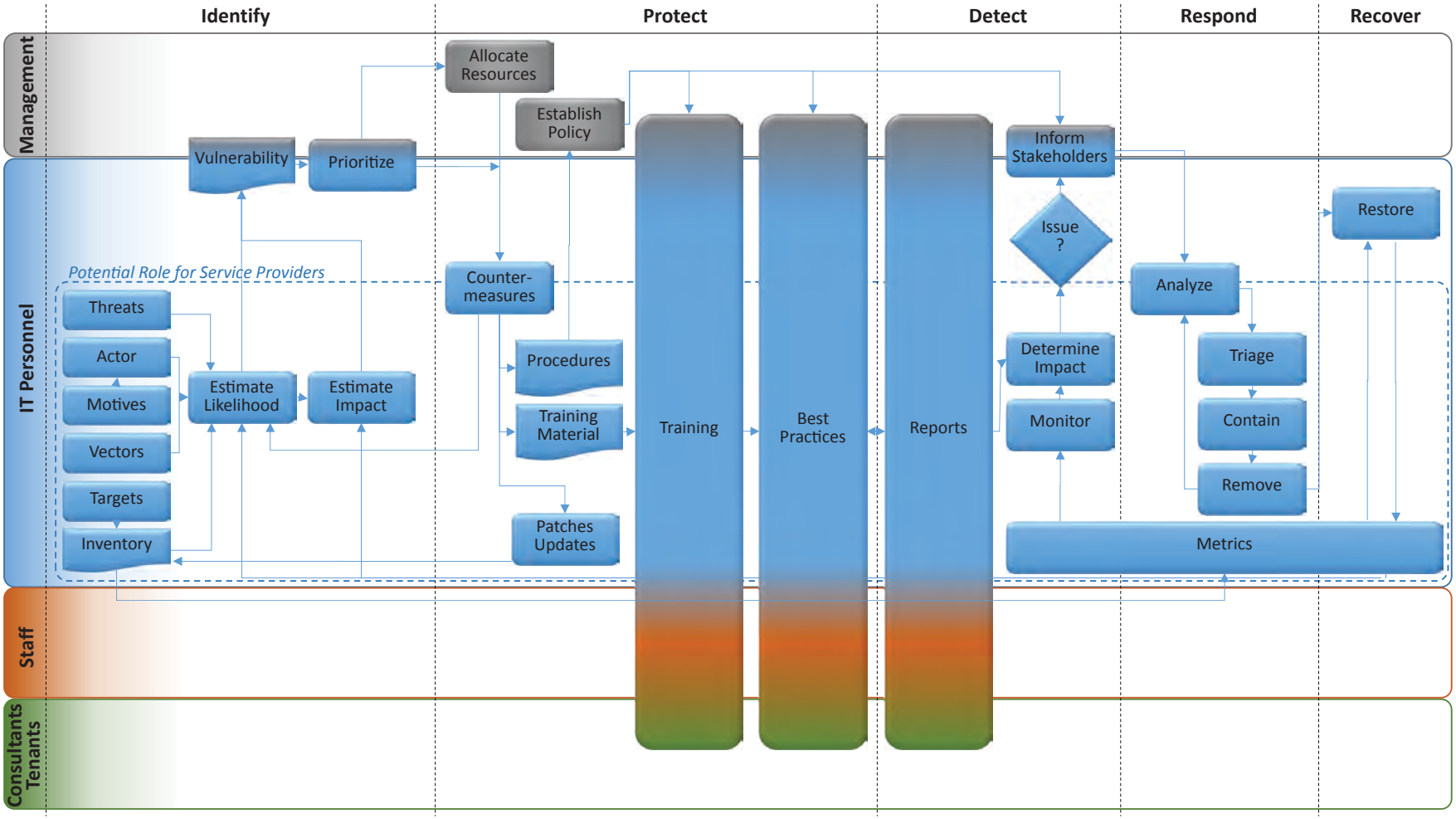


Figure 3. An approach to implementing cybersecurity at airports.

5. **Recover** from a cyberattack and update future response capabilities based on lessons learned. Backups of data and virtual system images can help in this regard. The goal is to return to a normal state of operation, but this requires a clear definition of what that normal state is.

Key Roles and Responsibilities

The five primary activities of the NIST Framework are carried out at an airport by senior management, IT personnel, airport staff, consultants, and tenants. Their roles are illustrated as the rows in Figure 3. These key roles are supported by a variety of other stakeholders from within the airport, as well as third party service providers. The manner in which each of these roles carries out cybersecurity activities is illustrated by the arrows in Figure 3. These primary and supporting roles are defined in detail in the Staffing section under Resources Required in Chapter 5 of this guidebook.

> An interactive version of Figure 3 is available in the multimedia material. This lesson on the process of establishing a cybersecurity program describes the overall approach to establishing a cybersecurity program and the key roles involved. Each step of the flowchart provides a link to further information about each step.

Cybersecurity Tasks

Within each of the five primary activities identified by the NIST Framework is a series of tasks that are carried out by individuals who fulfill the previously identified roles. These tasks are represented by the boxes in Figure 3 and are described in the general order in which they are carried out:

Identify

- **Threats** to an airport's data and systems exist and are increasing in number and sophistication. The first task for IT and facility managers is to identify threats that may impact airport data and systems.
- **Actors**, encompassing hackers, nation states, criminal organizations, and even insiders, will carry out cyberattacks against an organization by exercising a threat where they believe vulnerability exists. Actors should be classified based on their skill level, available resources, and motives. This information is referred to as attribution and can help in responding to and recovering from an attack.
- **Motives** are the reasons actors carry out threats. Knowing the types of motives (whether it is to obtain salable information such as credit card numbers, to disrupt operations, or to exploit sensitive information) can help when prioritizing countermeasures, as well as responding to and recovering from an attack.
- **Vectors** are the avenue or channel an attacker uses to conduct an attack. Identifying and understanding the possible vectors that an actor may use can help in assessing the likelihood of an attack.
- **Targets** of cyberattacks include IT systems and ICS, as well as the data contained within or conveyed by these systems.
- An **inventory** of the potential targets—including their criticality to airport operations; users served; vendors; software versions, patches, and updates; and data stored and exchanged—is essential information to a vulnerability assessment. This information can be collected during an IT master plan or other initiative but should be kept up to date as existing systems are reconfigured and new systems are installed. Maintaining a detailed configuration management database will make protection and detection effective.

- **Estimate the likelihood** of specific cyberattacks by reviewing the numerous combinations of threats, actors, vectors, motives, and targets that exist. The likelihood of these scenarios should be quantified to the extent possible. These quantitative rankings can be recalibrated over time as threats evolve, attacks occur, and lessons are learned.
- **Estimate the impact** of each vulnerability, should it be exploited by an attack, to determine the level of data, financial, or operational loss that could occur. Factors that should be taken into consideration include the impact to airport and National Airspace System operations; loss of personal, confidential, sensitive, or financial data that may occur; potential to violate regulatory requirements; number of affected users and stakeholders, as well as loss of reputation and public concern. The Cybersecurity Assessment and Risk Management Approach (CARMA) from DHS provides a methodology for assessing cybersecurity risks to critical infrastructure.
- **Vulnerability** assessments should summarize the threats to which airport data and systems are exposed, as well as the impact that a successful attack may have on data and systems. Vulnerability assessments may be carried out for all data and systems or for specific subsets deemed to be a higher priority.
- Senior management with the assistance of the CISO, as well as IT and facility managers, should **prioritize** vulnerabilities from those that should be addressed urgently, to those that should be addressed as resources are available, to those that are acceptable without mitigation.

Protect

- Senior management should **allocate funding and staff resources** based on the prioritization of vulnerabilities to be addressed, their tolerance for risk, and the availability of limited resources.
- **Countermeasures** should be led by the CISO and implemented by IT and facilities staff, possibly with the support of external providers, based on the priorities established and resources allocated by senior management.
- **Procedures** will be necessary to ensure that countermeasures have been properly established and are being carried out.
- **Policy** that is endorsed and enforced by senior management will be required to ensure procedures are followed.
- **Patches and Updates** to systems, especially those deemed essential from a security perspective, should be applied as they are made available by vendors. This process should be automated to the extent possible.
- **Training material** should be developed or procured to inform airport managers, staff, consultants, and tenants of their responsibilities with regard to implementing countermeasures.
- **Training** should be required of all staff, consultants, and tenants over which the airport has authority as a matter of policy. This training should be required of new hires and periodically of all staff, consultants, and tenants.
- **Best practices** that support the countermeasures employed by the airport should be carried out by all managers, staff, consultants, and tenants.

Detect

- **Reports** of anomalous activity of systems, suspicious human activity, and data breaches should be promptly communicated to the individuals responsible for cybersecurity at the airport. These reports may come through help desk personnel, managers, or security personnel.
- **Monitor networks** through software or hardware that is on-site or within data centers of external providers. Alerts of anomalous activity, attempted or unusual access requests, suspicious network traffic, or other events that may indicate an attack has occurred should be provided to designated IT personnel. Critical alerts should be conveyed to the CISO as soon as possible.
- **Determine the impact** of the reported activities and monitoring quickly using information collected and recorded in the inventory and vulnerability assessments.

- If an **issue** is detected, those responsible for cybersecurity at the airport should promptly take the appropriate actions.
- In accordance with the airport's communications policies, **inform stakeholders** who have previously been identified as being able to assist or who may be affected. Individuals responsible for cybersecurity should work with senior management as well as the communications staff to determine the appropriate content, timing, and distribution channel(s) of information regarding the cyberattack that has occurred.

Respond

- **Analyze** the attack to determine the severity of the impact, the cause, and the remediation actions that can be taken. The inventory, risk assessment, and metrics quantifying the normal state of operations should be taken into consideration.
- **Triage** should be conducted using the analysis described above as input to prioritize the actions that can be taken to react to the attack.
- **Contain** the causes and effects of the attack to the extent possible by quarantining malicious code, shutting down systems, closing network traffic, and other means. As these measures may affect legitimate and in some cases critical operations, backup procedures should be established so that they can quickly be implemented when needed.
- **Remove** the cause of the attack by deleting malicious code or rolling back systems to the last known stable state. The application of configuration management principles is critical for this to occur rapidly and efficiently.

Recover

- **Restore** data and systems to their normal state as quickly as possible. This requires that the normal state has been defined, which should be done as a part of the inventory process. Metrics should also indicate typical user loads and network traffic.
- **Metrics** should be tracked to quantify the effect of the attack so that lessons can be learned and used to re-prioritize countermeasures to reduce the likelihood of similar attacks occurring in the future, as well as to improve response to other attacks.

The activity areas, roles, and tasks described here and illustrated in Figure 3 form an approach to assessing and reducing the cybersecurity risks faced by airports. While this approach is founded on best practices, it is not the only option and should be adjusted to the needs of each airport based on its size, risk tolerance, and resources. Regardless of how cybersecurity is approached, the underlying goal should be to identify and address vulnerabilities to satisfy the risk aversion of senior management in an efficient and cost-effective manner.

Threats

Threats are actions that can adversely affect an airport's operations or assets (Committee on National Security Systems 2010). As airports increasingly use technology to support customer service (Ranasinghe 2014), improve aircraft operations (Port Authority of New York & New Jersey n.d.), enhance security (TSA 2014), become sustainable (Peters and Woosley 2009), and achieve many other strategic goals, they become more exposed to threats against their digital data and electronic systems.

Know your enemy . . .

–Sun Tzu

These cyber threats are increasing in number and in sophistication (Rainie et al. 2014). Individuals and organizations (aka actors) that are carrying out such attacks are also growing in number and sophistication. Nation states, organized crime, and corporations are investing substantial resources in cybersecurity offense. As the proliferation of interconnected electronic devices and the public's reliance on them grows, this trend is likely to continue.

An important first step in cybersecurity is to understand the type and sources of threats that airports face. As Sun Tzu, the ancient Chinese General, strategist, and philosopher, stated "Know your enemy" (Sawyer 2007). This does not mean that airports need to study every aspect of cyber threats, actors, and motives. There are agencies, companies, and individual consultants that are dedicated to this mission. Airports should, however, be aware of the resources that exist. These include agencies such as the Federal Bureau of Investigation (FBI), organizations such as MS-ISAC, and third party service providers. From these resources, airport CISOs should understand the threats that may expose vulnerabilities to their systems so that they can prioritize efforts to deploy countermeasures.

A place to start is with the NIST *Guide for Conducting Risk Assessments*, which identifies threats and organizes them into the following categories to facilitate the assessment of the impact they may have (NIST 2012):

- Confidentiality Breach
- Counterfeit Hardware
- Data Breach
- Delayed Technology Refresh
- Denial of Service
- Host Exploit
- Inadequate Monitoring of Events
- Ineffective Disposal
- Ineffective Testing
- Insider Threat
- Intentional Data Alteration
- Intentional Data Theft
- Internal Threat
- Labor Action
- Lack of Internal Control
- Malicious Code
- Organized Campaign
- Pandemic
- Phishing
- Physical Exploit
- Social Engineering
- Supply Chain Integrity
- Third Party Breach
- Unauthorized Access
- Unauthorized Host Access
- Unauthorized Network Access
- Unauthorized Physical Access
- Unauthorized Reconnaissance
- Unintended Data Compromise
- Unintended Data Leak
- Unpatched Hosts

Appendix A provides a more detailed list of the specific threats that fall into these categories.

There are hundreds of specific threats that airports should evaluate. Some noted by Bob Cheong of Los Angeles World Airports are distributed denial of service (DDoS), targeted botnet attacks, click-jacking, cross-site scripting, insider threats, and Trojan humans (Cheong 2011). This list and even the one in Appendix A are not comprehensive as new cybersecurity threats are constantly emerging. These lists, however, provide a place to start. A continuous process of scanning industry alerts and bulletins is also recommended.

Affected Data and Systems

The second step in an effective cybersecurity approach is to know what may be affected by successful cyberattacks. The second part of Sun Tzu's quote is to "know yourself."

. . . and know yourself . . .

–Sun Tzu

There is a broad variety of systems that can be adversely affected by the cybersecurity threats identified in the previous section. These systems encompass traditional IT infrastructure such as desktops, servers, and network devices, as well as ICS such as access control devices, heating and cooling controls, and baggage handling systems.

Systems that may be vulnerable are not just those connected to the Internet. As one interview respondent said, "if bits or bytes pass through it, it may be vulnerable." With the growing trend of employees using personal devices for work purposes and the proliferation of cloud-based

services, the systems that may be affected are not limited to those that the airport directly controls. Furthermore, with the implementation of the Federal Aviation Administration's (FAA's) Next Generation Air Transportation System (NextGen) Program, as well as the ongoing automation of aviation-related systems, the number of systems of concern to airports is growing.

Appendix B identifies over 200 types of systems typically found at airports that may be affected by cyber threats. These systems are grouped into the following 10 categories:

- Administration
- Airline & Airside Operations
- Cloud Based
- Development
- Employee Devices
- Facilities & Maintenance
- IT & Communications
- Landside Operations
- Safety & Security
- Tenant

Systems that are relevant to airports from a cybersecurity perspective can also be categorized by the domain in which they operate. The domain of the system, often but not always, is an indicator of who is responsible for the information that flows through it. Following are the primary domains of systems that should be considered when establishing a comprehensive cybersecurity program for an airport:

- **Airport IT infrastructure** encompasses hardware, such as computers, servers, routers, switches, and hubs; backend (e.g., database) and frontend (i.e., applications used by end users) software; network cabling, Internet connectivity, and security components; and humans including administrators, developers, and support staff (Janssen 2014).
- **Airport facility** control systems such as heating and ventilation control, airfield lighting, baggage handling, supervisory control and data acquisition (SCADA), and building control systems (BCS), and other ICS computers, devices, and cabling.
- **Employee devices** that airports may allow to be used for work purposes such as smartphones, tablets, laptops, computers (while working at home), and digital cameras.
- **Airline** ticketing, passenger processing, dispatching, crew scheduling, and aircraft operations. Some of these systems may utilize common use terminal equipment, common use passenger processing systems, common use self-service, flight information display systems (FIDS), and baggage information display systems that operate on airport-owned IT infrastructure. Even if airlines own and operate their own hardware and software, they may rely on airport network, Internet, and power connections. Some airlines may also use Avionics Full Duplex Switched Ethernet (AFDX®), engine health and usage monitoring systems, and electronic flight bags that at times rely on airport IT infrastructure (Roadmap to Secure Control Systems in the Transportation Sector Working Group 2012).
- **Non-airline tenants** may connect point-of-sale (POS) devices, parking access and revenue control systems, automatic vehicle identification systems, and other devices to airport IT, communications, and power networks.
- **Consultants and contractors,** whether they work on-site or off-site, may use airport-owned, company-owned, or personal devices that are connected to airport IT networks through VPN connections or other means. Even if not connected, they may transfer data onto the airport's network via universal serial bus (USB), portable hard drives, and other media.
- **Public** accessible Wi-Fi network connections, wayfinding kiosks, digital paging, and other devices are increasingly being made available at airports to improve customer service. All of

these devices are publicly accessible, by definition, and a surprising number are not secure. A study in 2008 of private (i.e., non-hotspot) Wi-Fi networks accessible within 14 airports around the world found 80% were unsecured or using flawed wired equivalent privacy (WEP) encryption. Some of these were used to support critical airport operation (Infosecurity Magazine 2008).

A conceptual diagram that highlights areas of a typical airport where cybersecurity is particularly relevant is provided in the multimedia material.

Both function and domain are important considerations when inventorying systems that may be affected by cybersecurity threats. To help assess the vulnerabilities that those systems may introduce and the countermeasures that can be employed to address them, airport IT managers, staff, or consultants responsible for cybersecurity should collect the following information:

- System criticality to airport safety and operational efficiency
- Ownership and maintenance responsibility
- Users and level of use based on granted access rights
- Make/model/version
- Configuration settings
- Communication protocols and ports utilized
- Status of patches
- Status of warranty
- Data considerations
  - Volume
  - Directionality of flow (to and/or from airport)
  - Requirement for create, retrieve, update, and delete privileges
  - Sensitivity, with special attention and handling given to SSI
- Airport and vendor point of contact

The data that passes through these systems is also important as it is often the ultimate target of cybercriminals. Data may include personal information on staff, tenants, and passengers; financial information; operational statistics; engineering drawings; procedures; and a variety of other documents. As part of the assessment of impacted systems, the sensitivity and confidentiality of the data stored and transmitted on those systems must be considered.

Ideally this information should be collected as a part of an airport's IT master plan, which will often include additional details relevant to the effective use and maintenance of systems at airports, such as useful life remaining and funding requirements (Purnell et al. 2012). These plans need not be complex and it is often helpful to organize the information characterizing each system in a tabular format for easy reference, ranking, and sorting.

It is recommended that IT master plans be updated every 24 to 36 months (Purnell et al. 2012). With the rapid evolution of cyber threats, this update cycle may be the longest limit airports should consider. That is, however, a decision airport management needs to make based on the relative costs and benefits of updating the master plan versus other activities competing for limited funds. Regardless of how often an airport updates its inventory of systems, it is recommended that systems be identified as they are installed, updated, or decommissioned so that the inventory remains as current as possible at all times. To accomplish this, the airport should establish a policy whereby all system changes are reported to the CISO before they are implemented.

The CISO or their staff and consultants should maintain this inventory of airport systems potentially affected by cyber threats. The categorized list of systems in Appendix B can serve as a checklist to help ensure all systems have been considered; however, the list provided should not be considered all inclusive as each airport may have unique systems and the range of systems in use by airports is constantly evolving.

Countermeasures

Precautions that can be implemented to protect an airport's systems against cybersecurity threats are referred to as countermeasures. They are controls that protect the confidentiality, integrity, and availability of data processed, stored, or transmitted by airport systems.

NIST 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* (Joint Task Force Transformation Initiative 2012), has identified, categorized, and prioritized cybersecurity countermeasures. They are grouped into three classes and 18 types as listed in Table 1. The classes correspond to the types of staff typically responsible for each type of countermeasure.

Appendix C provides a more detailed list of countermeasures based on industry best practices, NIST 800-53, and other material. Cross-references are provided to link each countermeasure with additional data in the NIST 800-53 document from which they came.

It is recommended that airports consider implementing countermeasures in a prioritized manner to address vulnerabilities that were identified during a cybersecurity vulnerability assessment. The NIST recommends that countermeasures be given one of three priority codes—P1, P2 or P3—and considered in that order. The assignment of codes does not provide a level of security; it only reflects the relative importance as chosen by the airport team. In the learning and recovery phase, these priorities may be revised.

While many countermeasures must be implemented by IT professionals, system vendors, and airport management, the cybersecurity program should educate airport staff, tenants, and consultants on the practice of good cyber hygiene habits. By incorporating these practices into

Table 1. Categories of countermeasures.

Class/Staff	Type
Management	Planning
	Program Management
	Risk Assessment
	Security Assessment
	System Services and Acquisition
Operational	Awareness and Training
	Configuration Management
	Contingency Planning
	Incident Response
	Maintenance
	Media Protection
	Personal Security
	Physical and Environmental Protection
	System and Information Integrity
Technical	Access Control
	Audit and Accountability
	Identification and Authentication
	System and Communications Protection

Source: Derived from Joint Task Force Transformation Initiative (2012).

their daily work life at the airport, an airport's vulnerability to a cyberattack can be reduced. The following list identifies good cyber hygiene habits:

- **Avoid Social Engineering Tactics**—Social engineering tactics are actions taken by adversaries to trick staff into divulging confidential information. Phishing emails that are constructed to appear as if sent from a legitimate source that prompt readers to click on a link or open an attachment are an example. All airport employees, consultants, and tenants should be aware of the most common social engineering tactics and learn how to avoid falling victim to them. This can be accomplished through training.
- **Create Strong, Protect, and Frequently Change Passwords**—Best practices for password management should be part of the ordinary habits for airport staff. For example, numbers and letters should be used in passwords that are difficult to crack but easy to remember. Passwords should also be changed on a monthly basis. They should not be written down and stored in conspicuous locations. Managers or staff overseeing the installation of a new system should check to ensure that default passwords set by manufacturers or installers are changed to strong passwords that are unique to the airport and comply with the airport's policies.
- **Identify Suspicious Behavior**—Any behavior that is out of the ordinary should be identified. This behavior may be actions carried out by other people, such as "shoulder surfing," i.e., looking over the shoulder of a user as they enter their credentials, and taking photos of computer screens or electronic devices. Suspicious behavior may also be seen in systems. Examples of such behavior, or anomalous activity, include web browsers showing content or redirecting to pages users did not request, applications returning information that is suspicious or not responding promptly, and abnormally slow computer performance.
- **Identify and Protect SSI**—SSI is a special class of information about physical security systems that must be protected as described in Title 49 of the Code of Federal Regulations (CFR), Part 1520. As part of this federal regulation, SSI must be labeled and handled appropriately. If airport staff, tenants, or consultants encounter SSI that they do not have rights to view and a current need to know, that information should be returned to the airport. If they do have permission and a need to know the information, then they should protect that information as required by airport policy. Communicating (and periodically reminding) employees and consultants of these responsibilities can be difficult, especially at larger airports. To help, some airports have incorporated SSI into their training programs and/or displayed posters in common areas.
- **Patch Personal Devices and Applications**—As BYOD to the workplace becomes more common, the burden of keeping those devices updated with the most recent versions and patches falls onto the staff member who owns the device. Many popular applications (e.g., Adobe Acrobat, Internet Explorer) are exploitation targets. Cyber criminals often develop code that tricks users into entering credentials or installing code that contains malware.

These and other daily best practices are described in more detail in the training section of the multimedia material.

CHAPTER 4

Implementing Countermeasures

The initial step to reduce cybersecurity risk is to identify the cyber threats that airports face and the data and systems that may be vulnerable to such threats. The next step is to protect those data and systems by implementing countermeasures that reduce the likelihood of a successful attack. This chapter provides details on some of the most important countermeasures and where within the airport environment they should be implemented.

Few organizations can implement all the necessary countermeasures at one time. Even if this were possible, a phased approach that addresses the highest priority vulnerabilities first is advisable. This priority should be established by assessing the likelihood of the vulnerabilities identified and the degree of impact a successful attack may have.

Once countermeasures are implemented, the job is not done. New systems are being implemented at airports at an increasing frequency; new threats arise daily; and countermeasures are rapidly evolving. This environment necessitates an ongoing, flexible, and adaptable approach to vulnerability assessment and countermeasure implementation. The sections that follow provide details on how to implement countermeasures to address common airport vulnerabilities.

Airport Systems

Most people are aware that cybersecurity affects traditional IT infrastructure such as desktop computers and servers as well as network devices such as routers and switches. Not as apparent are ICS that also can be vulnerable to cyberattack regardless of whether they are connected to the Internet. Wi-Fi networks used for public access to the Internet or secure airport operations also introduce unique vulnerabilities. Furthermore, airports are becoming increasingly reliant on the growing number of IT services that are in the "cloud," i.e., based within a third party data center that is accessed via the Internet. Airports, the FAA, and airlines are also increasingly reliant on GPS for operational safety and efficiency. Important cybersecurity considerations of these four domains of airport systems are discussed in the following subsections. Airport managers and staff—but also the external service providers who install, configure, operate, and maintain these systems—should review the countermeasures that are specific to the systems they implement. The software and data processes on these systems should also be sufficiently backed up and offer redundant capabilities, especially when they support mission-critical functions.

IT Infrastructure

Many are under the incorrect impression that, if IT infrastructure is not directly connected to the Internet, it is not vulnerable to attack. This perception is refuted by successful attacks that were initiated via portable storage devices such as USB drives, radio or infrared remote control devices, exposed connections to closed networks, and other non-Internet-based vectors.

While malware and virus attacks often manifest themselves on end points, they are carried, often stopped, and sometimes found on network devices. Some of the primary countermeasures that airports can take to protect their IT networks are as follows:

- **Physical protection** should be implemented to prevent criminals from gaining access to ports, cabling, and wireless devices. Within an airport, IT network infrastructure should not be accessible to passengers, the public, or airline and tenant personnel who have not been screened and perhaps badged by airport security staff. This means that this infrastructure should be installed in secure areas protected by access control devices, alarms, and, in some areas, closed circuit television (CCTV) cameras. Architects, design consultants, and construction contractors should be made aware of these requirements in bid packages, contracts, and specifications. If SSI is present in these documents, they should be labeled appropriately and circulated only to those who know their responsibility. Commissioning of the infrastructure should include checks to ensure that the proper physical security has been applied to protect network infrastructure. This will typically require support from IT personnel who are familiar with the topology (i.e., location and routing) of this equipment. More information on this physical protection can be found in countermeasures PE-1, -2, -3, -4, -6, -7, -8, -9 (Joint Task Force Transformation Initiative 2012), which are described in Appendix C.
- **Closing ports** is a way to halt some unauthorized internal and external data communications before it reaches a host system. Many applications rely on communications over specific ports (e.g., unsecured web traffic travels over ports 80 and 8080). Only ports that are required for authorized data communication over that branch of a network should be opened. This requires, as a part of the procurement process and software assurance process, that vendors identify required ports and that IT staff review these requirements before systems and applications are procured. Switching critical data communications to non-standard ports, if possible without affecting the functionality of the system or application being installed, is an added measure that may curtail attack vectors that target standard ports.
- **Malware-detecting** hardware and software can continuously monitor network traffic to identify known threats and/or anomalous activity, quarantine affected or at-risk systems, and alert personnel before the threat manifests itself in the network and eventually causes harm. As cybersecurity actors, threats, and vectors become more advanced and numerous, so have malware detection options. Many third party vendors offer solutions that range widely in price. Some of the more sophisticated options and services may only be feasible for larger airports, but there are also less expensive options that can meet the needs of smaller airports.
- **Backups** of system and data resources should be periodically and automatically prepared. Backups should be made before replicating the changes made since the last backup exceeds the cost of preparing a new backup. Because maintaining data can be laborious and therefore costly and the marginal cost of an additional backup is typically minimal, nightly backups are often commonplace. Virtual computing technology also allows full computers (i.e., operating system, installed software, and data) to be easily backed up and to quickly be brought online if an issue occurs. The media on which data and system backups are stored should be kept in a location that is secure from unauthorized access and physical damage by fire, flood, or other disaster.
- **Redundant capabilities** should be designed into the architecture of mission-critical systems. As with backups, the cost of a system's capabilities not being available for a period of time should be weighed against the cost of deploying redundant capabilities that can be accessed should the primary system fall victim to a cybersecurity attack.

Many other countermeasures can be implemented to protect IT network infrastructure. The Access Control, Physical & Environmental Protection, and System & Communications Protection countermeasure types listed in Appendix C are the primary ones for airports to consider and prioritize, although other categories offer countermeasures that may also help.

End-Point Systems

End-point systems include desktop computers, laptops, and tablets, as well as personal devices such as smartphones. Within an airport environment, FIDS, a tenant or an airport's POS devices such as parking payment machines, electronic kiosks, and visual paging devices can be considered end-point systems.

Protecting these end-point systems requires an understanding of their various components. First, there is the hardware itself. Next, there may be a basic input/output system (BIOS) or other types of firmware installed onto a chip within the system to control its basic functions. End-point systems also typically have an operating system to control more advanced functions. Applications are then installed that work with the operating system to provide functionality to users. These applications often rely on internal, or magnetic, or solid-state storage to store user data. Finally, there are input and output terminals on the system that allow data to be exchanged via a network or removable storage device. All of these components can be vulnerable to cyberattack and therefore must be adequately protected by implementing appropriate countermeasures.

Many organizations require end-point systems to have certain countermeasures in place before they are permitted to connect to the network. This requirement may be enforced by policies, procedures, and perhaps agreements between the airport and end users. These measures may also be automatically enforced by a network server or gateway host. If these requirements are not met, the machine may be isolated or virtually disconnected from the network (Rouse 2011). Some of the key countermeasures to consider when protecting end-point systems follow:

- **Physical protection**, meaning establishing tangible barriers such as walls, doors, and locks, should be implemented to protect end-point systems from unauthorized access. This includes keeping critical systems, data storage media, and network infrastructure within secured areas. It also includes securing devices in publicly accessible areas and protecting access to their ports and controls.
- **BIOS, firmware, and operating systems should be updated** to ensure that they have the latest protection prescribed by their vendors. Small, incremental updates that often address a specific issue are referred to as patches. The process of learning about and installing patches and updates can be complex and should be handled by qualified IT personnel. A patch management program is recommended and the responsibility to identify and install patches should be assigned to individual(s) within the IT department.
- **Antivirus and malware detection software** should be installed on end-point computers to detect, prevent, and remove malware before it is installed. Consultants and contractors should be required to have a certain level of malware detection software on the computers they connect to the airport's network, if such privileges are granted. All malware detection software should be kept up to date so that the latest protective measures are implemented.
- **Software assurance** processes should be established to ensure that all software installed on end-point systems employs a minimum level of countermeasures. The software assurance process is described in more detail later in this guidebook.
- **Legacy code should be eliminated or accounted for and tracked.** Many critical systems rely on software that includes older, i.e., legacy, code that was "secure at launch [but is] likely riddled with security holes today" (Marfatia 2014). As code or portions of it become inactive, that code should be removed from the application or system. If the code is still needed, it should be identified in the inventory of applications described previously. This will allow IT personnel to quickly identify attacks that target older systems. It will also support business decisions on where and when to invest in specific software upgrades.
- **Disabling USB ports** is a step several airports have taken to prevent the easy introduction of malware and theft of data. While this layer of protection can be beneficial from a cybersecurity

perspective, it does create an inconvenience to users, which should be considered as USB devices have become a common way of exchanging data.

- **VPN** software should be used to limit access within the airport's network when authorized users log in remotely. This limits the ability of attackers or malware to gain access to the airport's network by using the remote user's device as a conduit; however, this does not protect against malware that has already installed itself on the user's device, which is why virus or malware software should be installed on all end-point computers that have access to an airport's non-public network.

A wide variety of additional countermeasures can be employed to protect end-point systems. It is recommended that the System & Information Integrity and System & Communications Protection categories in Appendix C be reviewed for countermeasures that may be relevant to a particular airport.

Industrial Control Systems

ICS are systems used to monitor and control various systems such as airfield lighting, baggage handling, HVAC, and utility metering. SCADA, BCS, process control, industrial automation, and energy management systems are all categories of ICS that meet specific needs (Byres 2012). The majority of respondents [28 of 38 (74%) who answered the question] to the survey conducted for this project report that their organization uses ICS.

These types of devices increasingly rely on computer and network technology to collect data, analyze the information received, and react with corrective action. Many respondents [12 of 26 (46%) who answered the question] report that their ICS are connected to the Internet.

ICS, however, can also be vulnerable even if they are not connected to the Internet. Non-Internet attack vectors to ICS include removable storage used to update the firmware or applications on an ICS, compromise of sensors or communication cables linking sensors to control devices, remote control devices, and unprotected physical access to ports. ICS are also becoming increasingly interconnected and interdependent with other airport information systems, which may introduce additional vectors of attack. Because of this interconnectivity, these devices are exposed to similar vulnerabilities as computers and network devices. ICS and SCADA systems, however, also introduce additional vulnerabilities. The nature of their design requires distributed sensors and actuators that introduce vulnerabilities at these end points as well as along the conduit that leads to them. Unfortunately, malware detection software for SCADA systems is in its early stages, so the vulnerabilities of these systems are more acute.

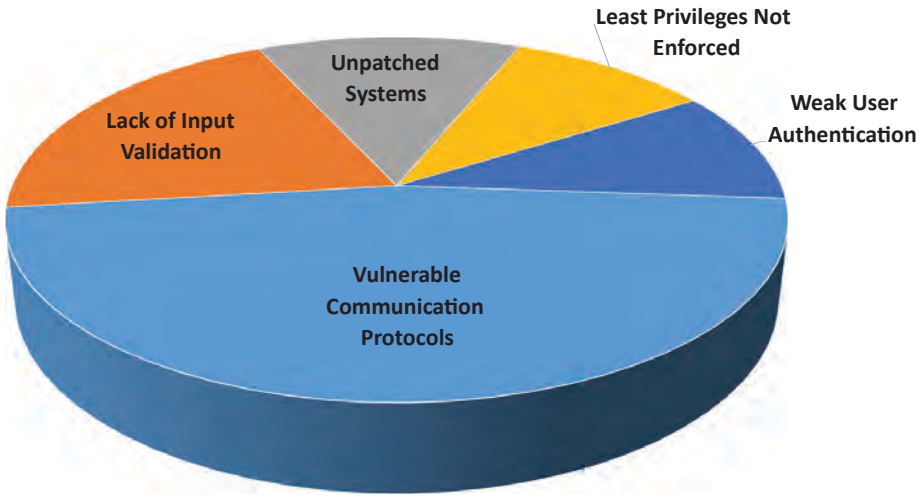
Distributed control systems (DCS) rely on control components spread throughout key nodes in an ICS network, such as a power distribution system. Other systems rely on programmable logic controllers (PLCs) or programmable automation controllers (PACs). These components are digital computers used for automation of typically industrial electromechanical processes, such as control of machinery or light fixtures. These logical units can be programmed to perform a variety of functions and report back to a common control system. PLCs and PACs can introduce vulnerabilities into an ICS because they are programmable and often lack the security features of authentication and physical protection that traditional IT computers include. In the past, these devices were considered embedded controllers and rarely communicated beyond their local system. Like almost all systems, they have grown in complexity and functionality and their vulnerabilities have increased as a result. Many now include programming ports, external network or wireless access for upgrade, monitoring, or configuration. In some cases the PLC may be used as a downgraded device without disabling of the communications links, leaving a vulnerability.

The problem is that cybersecurity best practices and countermeasures commonly applied to IT infrastructure have not been applied to ICS, although many are applicable. This is partially because these devices are often not considered vectors of cybersecurity attack and are therefore not always protected. Furthermore, vulnerability assessments and penetration tests are often not conducted on ICS (Gopalakrishnan et al. 2013). Many ICS and SCADA devices are based on older technology that is an easier target of modern attacks. To compound the problem, a recent study conducted by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) found that there is a lack of cybersecurity standards for protecting airport control systems (Kaiser 2012).

The growth of threats and the lack of countermeasures applied to ICS have opened up vulnerabilities that need to be addressed. Figure 4 shows the relative frequency of common ICS vulnerabilities. Other ICS vulnerabilities include unsecured databases, poorly configured firewalls, and interconnected peer networks with weak security. Many of these vulnerabilities are common to IT systems. Some vulnerabilities that have been identified as unique to ICS include heavy reliance on proprietary network protocols, undocumented software versions, lack of configuration documentation, and system stability variations during the vulnerability tests assessment (Gopalakrishnan et al. 2013).

The approach to implementing countermeasures to address ICS vulnerabilities is, at a high level, the same as that for traditional IT systems and network devices. The specific countermeasures that should be implemented may, however, differ. For example, many ICS devices that are accessible to the public require specific countermeasures to prevent unauthorized access or tampering. Others rely heavily on distributed sensors, which necessitates measures to protect the signals as they are transmitted to a central unit for analysis and action.

An important challenge to consider when protecting ICS devices is that they have typically not been considered a cybersecurity threat and therefore often have little or no security features. IT departments often responsible for cybersecurity are not always informed about ICS device installations until connections to the network or other IT resources are required. In many cases, ICS components may be installed and operational long before any consideration of cybersecurity. To overcome this challenge, facility managers who are typically involved in the specification, procurement, installation, and maintenance of these systems should work closely with the CISO, as well as other IT managers and staff as applicable.



Source: U.S. Department of Energy (2008).

Figure 4. Relative frequency of ICS vulnerabilities.

Recommended countermeasures for protecting the types of ICS devices found at airports include the following (adapted from Infrastructure Security and Energy Restoration Committee 2007):

- **Limit connections** to ICS so that only those that are needed are left open and those that are left open are properly secured. The very nature of ICS requires interconnectivity between dispersed sensors, control devices, control systems, and other components. This interconnectivity requires local and wide area network, wireless, Internet, or perhaps modem dial-up connections. This should include physical input/output ports on the components, as well as virtual ports that provide outside access to the network via firewalls. As a part of the inventory process, all required components, their connections, and protocols should be identified. Those that are not needed should be closed. Those that are needed should be secured using firewalls, de-militarized zones, intrusion detection systems (IDS), and other means. The goal should be to isolate the ICS as much as possible without limiting functionality.
- **Disable services** that are not required. Many ICS offer services such as automated meter reading, email notifications, and remote maintenance capabilities. These require network, and in some cases Internet, connections. As explained earlier, these connections can expose vulnerabilities. Services that are not required but are installed by default should be disabled.
- **Enable protective features**, which are often disabled by default to facilitate installation and maximize functionality. While older ICS may have few if any cybersecurity protective features, most modern ICS do. Unfortunately, malware detection software for SCADA systems is in its early stages.
- **Conduct vulnerability and penetration tests** on ICS as they are on IT networks. These tests should ensure that patches and updates have been applied, unused connections and services are disabled, and required functions are properly secured. Because ICS components are geographically diverse, a physical scan of all components should also be conducted to ensure that they are not accessible. Involve multiple stakeholders, including vendors, installers, users, and affected stakeholders, in a review of possible attack scenarios and the impact such attacks may have. This information along with the results of vulnerability and penetration tests will help prioritize the implementation of countermeasures to protect ICS components. Penetration testing is not recommended on ICS operating in a production environment due to the disruptions that can result (Dugan et al. 2005). Such tests can be performed prior to commissioning and operations or by tapping resources such as the National SCADA Test Bed (U.S. Department of Energy 2014).
- **Train facilities, as well as IT personnel**, on the importance of protecting ICS from cyberattack so that they are aware of and can accommodate proper countermeasures as a part of the selection and implementation of ICS. Staff and consultants who have access to data or components related to ICS should be aware of the sensitive nature of that information and protect it accordingly. As a matter of policy, all managers and staff responsible for ICS should be required to consult with the airport's CISO or designated IT staff member before the systems are procured and installed.
- **Include ICS in the inventory** of systems that may be vulnerable to cyberattack and in vulnerability assessments to be carried out on these systems.
- **Require strong user authentication** so that only authorized administrators, users, and maintainers can access ICS controllers and sensors. Caution should be taken so that their access is only to the system and components that they are responsible for and not to other components of the ICS or the network(s) to which it is connected. Passwords, often set to default values by manufacturers, should be changed upon installation and checked when the ICS is commissioned. User credentials should also be conveyed to authentication systems or transferred by administrators in an encrypted manner. Ultimately, user credentials for ICS should be subject to the same policies and procedures and credentials used for other systems.
- **Patch and update ICS.** This should be an organizational procedure that is assigned to a qualified staff member. Where possible, automated processes to install patches and updates as soon as they become available should be implemented.

- **Include ICS-specific cybersecurity assurances in ICS procurement requirements.** These include system configuration, physical access, authentication, system interconnectivity, malware detection requirements, and a variety of other considerations. Vendors should disclose any "back door" access points or default connections that may expose a system to cyber threat. Vendors should also provide documentation on what cybersecurity features are available and what default settings need to be changed to provide protection. The references below include two resources for ICS-specific procurement language.
- **Include ICS in incident management processes** and recovery operations. This includes establishing and informing points of contact among staff, affected stakeholders, and vendors prior to an attack and ensuring proper backups of data and that virtualized system components are up to date and readily accessible. With ICS, alternative processes and systems should be ready to activate should the functions of an ICS be unavailable as the result of a cyberattack.

Additional resources that airports, as well as vendors and installers of ICS at airports, may wish to consider include the following:

- Guide to Industrial Control Systems Security (Stouffer et al. 2013)
- National SCADA Test Bed (U.S. Department of Energy 2014)
- Cyber Security Assessments of ICS (U.S. DHS 2010)
- Cyber Security Procurement Language (U.S. DHS 2009 and Energy Sector Control Systems Working Group 2014).

Wi-Fi

Many airports offer public Wi-Fi Internet connectivity to passengers. A growing number are extending this capability to support baggage handling, aircraft gate, facilities maintenance, operations, and security needs. Wi-Fi has many of the same vulnerabilities as hard-wired network devices and introduces others because physical access is not required. Intercepting and stealing data, introducing service interruptions, and gaining unauthorized access to network system and data resources are among the threats that exist. Following are some countermeasures that can be implemented to reduce the likelihood of vulnerability to these threats (Wi-Fi Alliance 2015):

- **Change default administrator credentials** on Wi-Fi network devices.

For non-public Wi-Fi networks implement the following countermeasures, as well:

- **Enable Wi-Fi protected access** (WPA2) pre-shared key (PSK) security with advanced encryption standard (AES) encryption.
- **Create strong** network **passphrases**. Enable WPA2 security on client that users will use to access Wi-Fi devices. These passphrases should adhere to the airport system's credential policies where applicable.
- **Secure ports** on public Wi-Fi networks so that users can only access the ports and protocols granted by the airport. This may mean only granting access through port 80, which is the most common port used by the hypertext transfer protocol for website traffic. The airport may decide to open other ports to allow secure sockets layer (SSL) protocol for encrypted information that most sites use to handle personal or confidential data (e.g., to process credit cards as passengers change their airline reservations). Airports may also wish to open ports used by businesses for VPN or remote desktop connections. The more ports that are open, the more services are available to legitimate users, but also the more vulnerabilities are exposed to cybercriminals. This tradeoff between service and protection is a decision each airport that offers a public Wi-Fi network must consider.
- **Segregate public Wi-Fi networks** so that attacks that successfully overcome the previously described countermeasures can be isolated to the publicly available network so that they do not infiltrate the airport's private network.

When airport staff and consultants use public Wi-Fi while traveling for work purposes, they should be instructed to take the following precautions:

- **Enable WPA2 security**
- **Disable automatic connections to new networks**
- **Disable file and printer sharing**

These basic precautions and others should be reviewed with IT service providers that install Wi-Fi network devices at airports. Security requirements should be considered as a part of the network design and should be required by contract. Airport IT staff that work with Wi-Fi network devices should be trained on Wi-Fi security best practices.

Cloud-Based Services

Airports are progressively relying on servers, software, and data that reside outside of their network and are accessed via the Internet. This trend is so pervasive that Gartner, Inc. (2013) predicts spending on cloud computing will represent the bulk of overall IT spending by 2016. Ed Anderson, research director at Gartner, suggests that the "growth in cloud services is being driven by new IT computing scenarios being deployed using cloud models, as well as the migration of traditional IT services to cloud service alternatives."

Examples of this shift can be found among airports as well as the FAA. One large hub airport interviewed is relying on cloud services to support email and general office (e.g., word processing, spreadsheets, presentations) software needs. The FAA is also headed in this direction with a contract to move 60,000 users to Microsoft®'s cloud-based Office 365 for email, messaging, teleconferencing, and other office applications (Battey 2014). In support of NextGen, the FAA is also considering hosting weather processing services in the cloud (Marks 2013).

These organizations and others are tapping the resources of cloud computing for a variety of reasons. Airports interviewed for this project state a key appeal of the cloud is the ability to tap services without the cost and time required to establish those same services internally. Vendors interviewed for a related ACRP project (11-03, Topic S03-07, "Integrating Airport GIS Data with Public Agency GIS") noted that cloud computing allows them to deploy the latest software releases and provide maintenance that serves all of their customers without the burden of distributing media one customer at a time.

Because cloud computing resources are so readily available and are outside of an airport's firewall, some airport staff members interviewed feel that they fall outside the purview of their airport's IT policies and procedures. Other respondents, typically CIOs or CISOs, feel that their responsibility is to protect an organization's data regardless of whether it resides on internal IT infrastructure or in the cloud. This more inclusive perspective seems to be a growing trend. These differing perceptions are enabled by a general lack of cloud computing policy and procedures for end users to follow. Regardless of an airport's position on cloud-based computing, policy and procedures that define how its staff should approach and interact with cloud-based services are a growing necessity.

Cloud computing exposes an airport to similar threats as internal systems expose, except that cloud computing services are available on the Internet and the airport is not directly in control of the countermeasures that can protect these resources. Fortunately, data on the cloud can be protected, but it is exposed to governments, criminal organizations, hobbyist hackers, and others (Honorof 2013a). The National Security Agency, through its PRISM program, has partnerships with many leading cloud-based providers that enable them to access the private data these providers host for their customers (Honorof 2013b). Some providers offer encryption and do not store user login credentials (Honorof 2013b). A study by Johns Hopkins noted, however, that

data that is encrypted at the cloud provider's site may be visible. Access credentials, if established via a web portal, may also have been intercepted or falsely generated by "man-in-the-middle" attacks (Butler 2014). Recommended countermeasures for airports that use or are considering cloud-based computing services are as follows:

- **Identify and document requirements** for security, privacy, and other organizational needs for cloud services (Jansen and Grance 2011).
- **Perform a risk assessment** of identified cloud computing requirements (Jansen and Grance 2011).
- **Develop policy** governing the use of cloud-based computing.
- **Implement a procurement process** for selecting and evaluating qualified cloud service providers (Jansen and Grance 2011). The following steps are recommended:
  - Evaluate a cloud provider's ability and commitment to deliver secure cloud services. Periodically assess their capabilities because the threats facing cloud computing, as well as the capabilities of providers, are rapidly evolving.
  - Ensure that all contractual requirements are explicitly recorded in a service-level agreement (SLA) with the cloud services provider. Involve a legal advisor to review the SLA.
  - Prior to sharing data resources, confirm that the cloud service provider will return and not store copies of the airport's information upon termination of the SLA.
  - Refer to (if available) or conduct (if feasible) a third party risk assessment on the selected cloud provider's infrastructure.
  - Ensure that any relevant code or encryption keys are escrowed with a trusted third party.
- **Only send encrypted data** into the cloud, because data in transit can be intercepted and, if not encrypted, can provide attackers with credentials and sensitive information. Often this information can be used to give them a higher level of access for subsequent attacks. Data is encrypted when transferring data using SSL, but an added precaution that should be considered where possible is encrypting the data using a secure key before it is transferred.
- **Use a desktop application to transfer files** instead of doing so through the cloud provider's web portal (Butler 2014).
- **Follow the cloud provider's security procedures and protocols**, which are often readily available on the cloud provider's site or can be requested. Some cloud providers publish best practice guidelines for their clients to use when transferring data or implementing systems on their infrastructure.

Global Positioning System

GPS technology is increasingly being used to support aircraft navigation and position reporting, airport vehicle and staff routing, and other activities at airports. While some of these uses support the airport, others that support FAA and airline operations can also influence airport operations. Unfortunately, GPS service can, and has at airports, been disrupted (i.e., GPS positions are temporarily or permanently stopped) or spoofed (i.e., intentionally false signals that lead to inaccurate positions). Executing these threats requires knowledge, equipment, and nearby access to those devices. Many actors have or can easily learn these techniques, acquire inexpensive equipment, and get close enough to airport GPS equipment to cause harm. Some may not be intentionally trying to interfere with the airport but inadvertently do so while nearby.

Human Considerations

Often cybersecurity is viewed as a technical challenge involving complex software and hardware configuration and review of extensive logs of network activity. While these are important elements of a cybersecurity program, the majority of successful attacks have been the result

of human action or inaction. "In most cases, negligence is the source of a breach. It's not that there's a malicious outsider colluding with a malicious insider, it's that there's a malicious outsider who's figured out how to take advantage of employee error," notes University College London Research Institute in Science of Cyber Security director Angela Sasse (Stapleton 2014). Unwittingly opening a malware attachment, being lax about protecting SSI, poor protection of passwords, and posting inappropriate information on social media have all led to successful cyber attacks, many at airports.

95% of security incidents investigated by IBM in 2013 involved human error.

–IBM (2014)

Training to increase awareness of these threats and measures that airport staff can take to avoid them is provided in the multimedia material.

While such human actions are sometimes unavoidable, many can be avoided by providing training, establishing and enforcing policy, and encouraging proactive reporting. Fortunately, these countermeasures are relatively easy to implement and there are many resources available to help. The ease of implementation and the potential to lower the percentage of successful attacks suggest that human-related countermeasures can provide a high return and should be among the first priorities of a cybersecurity program. The most common threats related to human activity and the countermeasures that can be implemented to reduce their likelihood are described below.

Social Engineering

Social engineering is the use of tools and techniques to trick legitimate users into disclosing confidential information. Often this information is used by criminals to gain access to sensitive data or critical systems. Sometimes this is achieved by tricking a user into installing malware that can support other more advanced attacks. The following are commonly used social engineering techniques:

- **Phishing** is sending emails to trick recipients into divulging information or clicking on a link. Attackers may pretend to be in need of immediate help and target the better nature of people trying to respond to emails with confidential information. Spear phishing is a special type of phishing targeting specific individuals with elevated access rights or decision-making authority. For example, an actor may obtain information from a public or compromised source, such as a supervisor, senior manager, or trusted organization. They then use this information to send what appear to be legitimate emails to individuals within the targeted organizations.
- **Smishing** is similar to phishing, but uses text messaging to phones, tablets, or other devices.
- **Vishing** is similar to phishing, but uses voice or telephony devices such as phones.
- **Shoulder surfing** is when actors look over the shoulder of an unsuspecting individual as they are typing a password or an access code into a keypad. Some sophisticated actors use long-range cameras and may even work in teams to accomplish their goals.
- **Dumpster diving** is when actors search trash cans and recycling bins to obtain sensitive or confidential information. Actors often look for information like remote access software used and configuration rules so they can profile software vulnerabilities to plan a more aggressive attack. For example, SSI should be shredded (ideally cross shredded) before it is thrown away.
- **Survey participation** is when individuals are enticed with the promise of prizes and other rewards to fill in an online survey that appears legitimate but is actually collecting information that can later be used to support an attack.

Attackers often exhibit some common traits, of which legitimate users should beware. These behaviors include the following:

- Avoiding conflict by using a friendly approach rather than an aggressive one.
- Attempting to develop and build a relationship through previous dealings.
- Quick willingness to compromise.
- Attempting to distance any responsibility from the target so the target is not hesitant.
- Making the target feel guilty.
- Misspelling words or making grammatical mistakes in emails allegedly from sources that would not make such mistakes.
- Being brief, when the source would typically provide more detail in the context of the email (e.g., simply saying "check out the attached" without any context or description).
- Sending email from addresses that do not appear to have originated from the source claimed in the text of the email.

Countermeasures that can be put in place to reduce the likelihood of a successful social engineering attack include:

- **Provide training** to increase awareness of social engineering tactics and the possible signs of an attack.
- **Encourage employees to report suspicious behavior** from either humans or computers. They should be warned to not intervene in an active crime but to report their observations as quickly and as safely as possible to security and/or law enforcement personnel.
- **Intentionally send out fake phishing emails** to staff that resemble a real phishing attack. When staff members respond to the email, debrief staff to provide additional instruction and guidance so that the mistake is not repeated when they receive a real phishing email.
- **Implement malware detection software** that quarantines or alerts recipients to questionable emails.
- **Block domains and email addresses** of known attackers before the emails are received.

These countermeasures can be very effective in reducing the likelihood of successful social engineering attacks; however, no protective measures are 100% effective. This is especially the case where the variable of human nature is a factor. Even a staff member who is familiar with social engineering tactics may be distracted or tricked by a particularly convincing phishing email. Organizations must also be prepared to respond and recover when a social engineering attack is successful. In addition, software should be put in place to detect anomalous activity quickly and end-point protection should be in place to isolate the effects as much as possible.

An explanation of social engineering tactics to avoid is provided in the multimedia material.

Bring Your Own Device

Increasingly employees are bringing their own smartphones, tablets, laptops, and other devices to work and using them in some cases for business purposes. This trend has become so pervasive that some analysts estimate that 40% to 75% of organizations have adopted BYOD (Phifer 2013). Some airports have also embraced this trend.

Many reasons are behind the trend toward allowing BYOD. Personal devices reduce the cost of hardware, software, subscriptions, and network charges. Employees are also familiar with the device(s) they have selected, which can reduce training costs. Empowering employees to select

their own devices that are best suited to their needs can also boost productivity. As with rental versus personally owned cars, users are more likely to treat their own equipment better (Citrix 2012).

Despite the benefits, many airports choose a more traditional approach of banning employee-owned devices from their network or workplace altogether. Such a strategy is understandable, as the NIST cautions "organizations [to] assume that all mobile devices are untrusted unless the organization has properly secured them and monitors their security continuously while in use with enterprise applications or data" (Souppaya and Scarfone 2013). That said, the popularity of mobile devices is an overwhelming trend. The use of mobile devices grew at a rate of 115% in 2013, led by messaging and social media applications, claims Flurry Analytics (Khalaf 2014). "Simply banning BYODs from the workplace rarely works," suggests Lisa Phifer of Core Competence, Inc. (Phifer 2013). Supporting this notion, Dave Martin, vice president and chief security officer of EMC, challenges "anyone who says they don't have BYODs to review their logs—I guarantee they'll find Mobile Safari."

"Simply banning BYOD from the workplace rarely works."

–Lisa Phifer of Core Competence, Inc.

Whether airports welcome or acknowledge BYOD use, it is prudent that they implement countermeasures to protect their organizational data and systems. This is challenging because personally owned devices introduce some new threats, including the following:

- **Less than 25% of stolen or lost devices can be remotely wiped** to ensure no sensitive or confidential data is lost, states the Security for Business Innovation Council. Dave Martin of EMC notes, "when email is retrieved and opened on a BYOD, I lose visibility into data access. In a phishing attack, I have no idea it even happened, and I lose any chance of [forensic investigation]" (Phifer 2013).
- **BYODs often bypass inbound and outbound security filters** enforced by network devices. This can expose the devices to malware and risk non-compliance with data privacy and regulatory requirements (Phifer 2013).
- **Downloading and installing applications is less regulated** on employee-owned devices (Phneah 2013).
- **Former employees may forget or intentionally not disclose** that they have corporate information on their personal devices, which then leaves with them (Phneah 2013).

To protect airports from threats introduced by personally owned devices in the workplace, the following countermeasures should be considered:

- **Establish a BYOD policy** to protective sensitive information on employee-owned devices. This should be an amendment to an acceptable-use policy for computers and organizational data. A BYOD policy should include the following:
  - Indicate which employees are eligible to use personal devices in the workplace (Citrix 2012).
  - Clearly articulate the delineation between personal and airport business.
  - Establish a list of allowed devices and operating systems.
  - Identify the types of applications permitted for work use on employee-owned devices.
  - Identify the types of airport and personal data that should be accessed, used, and stored on the device. This is particularly relevant with regard to data protected by laws and regulations.
  - Establish legal and copyright protection for airport-owned data.
  - Establish the right to review any email or, at least any airport-related emails and data on the BYOD. Privacy laws must be taken into consideration when employee personal and work-related emails are co-mingled.
  - Indicate which device maintenance activities are the responsibility of the owner and which the airport will support.
  - Indicate the responsibility to report the device is lost, stolen, or replaced.
- **Check compliance** with the BYOD policy by periodically asking employees to renew their agreement to adhere to the airport's BYOD policy.

- **Scan network** logs to determine if mobile devices are being used. If so, determine if they were used in appropriate ways.
- **Protect credentials** to airport systems that are entered into the employee's device, so that they are not cached, stored, or persisted. Instructions on how employees can implement this countermeasure should be a part of an employee training program.
- **Require VPN** connections be used that limit access to external sites while the employee is using their device for work purposes.
- **Encrypt data** exchanged between the employee's device and airport systems.
- **Implement software** that helps provide secure access to airport data and systems and can manage the applications and data on personally owned devices. Wireless intrusion prevention systems, mobile device management (MDM), and network access control systems are common technologies used to help protect a network from threats introduced by mobile devices (AirTight Networks 2012). One airport interviewed has employed MDM technology in conjunction with VPN access to allow employees to use their own devices while working on the airfield for facility, operations, and maintenance purposes.
- **Enforce exit policy and procedures** that require departing employees to remove applications and credentials that provide access to data and systems and all corporate data. An acknowledgment form signed by the former employee may dissuade many from violating these procedures (Citrix 2012).
- **Train employees** on the risks associated with using their own devices and on the airport's policy, procedures, and resources associated with such use (Lofgren 2013). Employees must understand their responsibility with regard to using their own devices in the workplace.

Embracing, or at least addressing, the BYOD trend is really not an option.

Embracing, or at least addressing, the BYOD trend is really not an option: it is a necessary element of a comprehensive cybersecurity program. Implementing the previous countermeasures may not only help protect an airport but may open up productive uses of personal devices, improve productivity, and enhance morale at a reduced overall cost of ownership. These benefits, however, must be weighed against the cost of implementing and maintaining the proper countermeasures.

Training for employees on BYOD is provided on the multimedia material.

Use of Social Media

Social media are becoming an effective and pervasive professional tool. Social media encompass the following:

- Content on a publicly available website
- Entries on weblogs (aka blogging)
- Posts on Facebook™
- Twitter™ tweets (aka posts)
- Announcements on LinkedIn™
- Live video streaming or "livecasting"
- Really Simple Syndication (RSS) feeds

For airports, social media can be an effective way to communicate information about airport services, upcoming projects, and opportunities for local businesses and consultants. Social media can also be a helpful tool for airport marketing, air service development, and collecting information on customer service and traveler experiences.

Social media, however, introduce a means of exposing information that, in some cases, should be protected. The use of social media in the work place also introduces additional cybersecurity risks that need to be considered. Some of the most common risks are as follows:

- **Decreased productivity** can result from the use of social media. This is not necessarily a direct threat to security, but it is an important factor. From a cybersecurity perspective, a distracted staff member is also more likely to fall victim to social engineering attacks. Also, if the airport allows employees to use their own devices in the workplace, they may be more inclined to use social media applications and managers may be less able to monitor the increased use of social media and its risk.
- **Malware and viruses** are typically propagated via email or Short Message Service (SMS) and can be served using social media exchanges via hyperlinks or email.
- The **spread of erroneous information** can help criminals introduce panic, confusion, and other factors that can help their attack. Social media are also increasingly used to recruit supporters of nation state and terrorist motives.
- **Leakage of sensitive or confidential data** on social media sites allows adversaries to gain information that they then use for spear-phishing attacks. In some industries, cyber intelligence monitors scan social media sites for publication of confidential information.
- **Reputation can be adversely affected** by disgruntled employees publishing rumors or false information about airport safety records, airline practices, and other areas of interest to the public.

To reduce the likelihood of social media threats, the following countermeasures should be considered:

- **Address social media use in policies and procedures.** Use of social media and its risks should be part of an acceptable-use policy. Airport staff must be aware of the effect of their actions on their employment as well as the potential safety and security impacts on them, their airport, and the public. The use policy must be prescriptive and specific so there is no ambiguity of the acceptable use of social media.
- **Monitor and control the content that is posted.** Management should not assume that airport staff have read the policy but should upgrade their content monitoring and technical controls as well as their network monitoring capabilities to scan for inappropriate use of social media.
- **Provide training to increase awareness of social media threats.** An effective way to remind staff members of the dangers and risks of using social media is by constantly updating and requiring training on the acceptable use of social media and the airport's social media policy. Training should highlight the social media risks with real life examples and provide education on corrective actions for abuse and non-compliance of the social media policy for employees.

Illustrations of social engineering tactics along with real examples of phishing emails to avoid are provided in the multimedia material.

Malicious Insiders

A malicious insider threat "is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems" (Carnegie Mellon University 2014a). This differs from unintentional insider threats where staff members, consultants, and tenants fall victim to social engineering tactics, mishandle sensitive data, or

allow their system credentials to be stolen. Such unintentional behavior can be addressed by providing training and enforcing policy. Intentional violations warrant punitive action and may be met with fines, penalties, termination, and other legal action. Malicious insider threats are more difficult to mitigate for several reasons. They originate from actors who have a higher degree of access than outsiders. These actors are also familiar with the vulnerabilities and critical data and systems of the airport. They are less easy to be detected because they often have a legitimate reason for accessing sensitive data and systems. Recommended countermeasures that can be taken to protect an organization against insider threat include the following (Cappelli 2012):

- **Communicate across departments**—including senior management, human resources, IT, security and legal—about general threat concerns, specific employees to be watched, and policy and procedures that should be carried out. This sensitive information should be conveyed based on protocols outlined in the airport's communication policy.
- **Monitor behavior** of employees, consultants, and tenants that are disgruntled, have a history of malicious behavior, or may have sought employment solely to gain a higher degree of access. While doing so, care must be taken to abide by employee privacy laws, regulations, and policy.
- **Collaborate with Human Resources** to determine which employees may be likely to become threats and monitor their data, computer, and network activity. They may include employees that are not performing to expectations, those likely to be laid off or terminated, and those recently passed over for a raise or promotion. Also, work with Human Resources to incorporate cybersecurity best practices into a workplace violence program.
- **Leverage technology** by monitoring incoming and outgoing data via an IDS, check for abnormally high volumes of data movement, and create signatures in security information and event management systems, which can log and monitor for suspicious activity. Focus and protect the most critical data and systems identified during the inventory of data and system vulnerabilities.

Additional resources that may help airports identify and mitigate malicious insider threats include the following:

- ***CERT Guide to Insider Threats*** (Cappelli et al. 2012)
- ***Common Sense Guide to Mitigating Insider Threats*** (Silowash et al. 2012)
- ***Bridging the Gap: A Pragmatic Approach to Generating Insider Threat Data*** (Glasser and Lindauer 2013)
- **"Insider Threat Test Datasets"** (Carnegie Mellon University 2014b) is a series of datasets on malicious actors and related background data

Service Providers

Many types of organizations provide services to or at airports. From a cybersecurity perspective, these providers fall into the following two categories:

- Those that can increase the likelihood of a cybersecurity attack
- Those that provide products or services expressly to reduce that likelihood

These groups need not be mutually exclusive; in fact, the greater the overlap, the better, as explained in the following sections.

Service Providers That Can Increase the Likelihood of a Cyberattack

Airlines, concessionaires, ground transportation providers, emergency responders, and consultants all provide services to or at airports. In the course of providing these services, they may have access to information or systems in a manner that can increase the likelihood of a cyberattack.

A distinction can be made between organizations that provide services to airports (e.g., consultants) and those that provide services at airports but are not engaged by the airport itself (e.g., emergency responders). While this distinction is relevant, because it may limit the types of countermeasures the airport may enforce, the primary question to be asked is what level of access these providers have to data and systems that the airport is responsible to protect from cybercrime. This question can be answered when developing an inventory of data and systems during a vulnerability assessment. During the inventory process, those providers who have direct or indirect access to data or a system should be identified. Once identified, the following countermeasures should be considered to properly protect airport data and systems from service providers:

- **Data and system use agreements** should be signed by service providers that have access to airport network resources. This should include an acknowledgment of SSI and how it should be handled as well as an affirmation that airport data and systems will be used only for airport business and in accordance with the airport's acceptable-use policy.
- **Cybersecurity training** should be required as a part of contracts, lease agreements, and operating permits of service providers engaged by the airport. The level of training should be adjusted to the degree to which the provider has access to an airport's network resources. For example, a janitorial services contractor should be provided basic awareness training and instructions on how to report suspicious activity. A consultant providing IT services will require additional training on how to access, use, and protect network devices in the course of their work at the airport.
- **IT protocols and procedures** should be established for consultants and other providers of IT or communications services to the airport.
- **Software assurance** procedures should be required of all consultants and vendors who implement systems for the airport. Defined procedures should include both software and hardware systems, and procedures on systems implemented on airport premises as well as in the cloud.
- **Certification** of vendor capabilities to support countermeasures should be considered as a means of ensuring that the vendors maintain the staff, equipment, and procedures needed to support the airport's cybersecurity requirements. Certifications should be periodically renewed with vendors that provide information or systems on a multi-year basis.

Service Providers That Help Protect an Airport

Service providers continue to emerge (and evolve) in response to growing threats and the resulting increase in demand for cybersecurity services. The result is a myriad of options for an airport to consider that span all steps of the cybersecurity process. While some of these services are free, others can be expensive. Some services are offered in conjunction with hardware and products. Some are to be implemented once, while others are periodic or continuous. While the landscape of these offerings is constantly changing, following are some of the most prevalent current offerings:

- **Awareness and training** materials are being offered by a growing number of government, non-profit, and for-profit entities. This guidebook and the accompanying multimedia material are examples. The PCI-Essentials online training courses offered by the PCI Security Standards Council is another example. Additional courses can be found at www.pci-essentials.com. The Texas A&M Engineering Extension Service's National Emergency Response & Rescue Training Center also offers a series of free cybersecurity awareness, planning, and management courses online at https://teex.org/Pages/homeland-security.aspx.
- **Vulnerability assessment** specialists working for large organizations, independent consultants, and even non-profit organizations can assist airports in identifying data and system

vulnerabilities, as well as assessing the likelihood of these vulnerabilities occurring and the impacts they may have. Such specialists can also help an airport prioritize the implementation of countermeasures to address these vulnerabilities. DHS, working in conjunction with ICS-CERT, NIST and others, have developed free tools and adaptable approaches that organizations can use to assess vulnerabilities and set priorities for implementing countermeasures. For example, CARMA from DHS provides a methodology for assessing cybersecurity risks to critical infrastructure. The Cyber Security Evaluation Tool (CSET) helps organizations evaluate their cybersecurity risk posture.

- **Information sharing and analysis centers** (ISACs) play an important role in sharing information on threats as well as connecting organizations with service providers that can help prevent and respond to attacks. Two ISACs that are particularly relevant to airports are the MS-ISAC and the Aviation ISAC (A-ISAC). Both of these centers provide information on threats and points of contact free of charge to airports.
  - **MS-ISAC** offers members cybersecurity threat briefings, advisories, and alerts; best practice tips and training material; lists of attackers; a tool for analyzing malicious code; and newsletters. For an additional fee, more advanced services such as vulnerability assessments, network monitoring services, and incident response assistance are provided. Several airports are already members of the MS-ISAC, which is considered by the DHS to be a "key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments" (MS-ISAC, 2014).
  - **A-ISAC** provides indicators and warnings of cyber and physical threats relevant to the aviation sector; offers a central resource for the sharing of best practices relevant to airlines, aircraft manufacturers, airports, and other aviation stakeholders; coordinates law enforcement activities related to aviation cybersecurity; helps coordinate attack response and recovery activities within the aviation sector; and interfaces with government agencies and other sectors. It acts as a neutral and trusted resource to receive, filter, and disseminate information to stakeholders. Its mission is to "reduce risks and costs associated with disruption to aviation operations due to cyber & physical security events" (Francy 2014).
- **Network monitoring** is a collection of systems, processes, and people that work together to monitor inbound and outbound network traffic. The primary task is to review network logs (e.g., proxy logs, application and host logs) for anomalies and take action on relevant alerts. Systems monitored include, but may not be limited to, firewalls, IDS, and intrusion prevention systems. Often the cost of in-house network monitoring can be excessive for an airport. In these cases, off-site service providers can offer some level of protection at less cost.
- **Automated alerts** are system-generated notifications that provide information about possible threats as they occur. Because of the volume of information reviewed, it is important that airports roll out an efficient and reliable process to configure and continuously fine-tune such alerts. The basic strategy is to minimize false positives and maximize relevant alerts. Achieving this goal requires a constant tuning process that is triggered by changes to the cybersecurity threat landscape, updates to software and hardware, as well as changes to business requirements.
- **Local and regional law enforcement agencies** are becoming increasingly prepared to help airports within their jurisdiction by sharing cyber threat information, assist with implementing countermeasures, and provide support if an attack does occur. As a part of an effective cybersecurity program, points of contact at these agencies should be identified, briefed, and kept informed about airport cybersecurity matters on a regular basis. The appropriate law enforcement authorities should be notified if an attack occurs.
- **Federal agencies** such as the FBI have field agents that are assigned to airports and can be a conduit for assistance from the FBI and other agencies if an airport cybersecurity attack does occur. To be the most effective, the agents assigned to an airport should be identified, briefed, and kept informed about airport cybersecurity matters on an ongoing basis through continued contact between the airport and the local FBI office.

The choice as to which and how many of these service providers should be tapped is a decision each airport's management needs to make based on the relative cost versus the benefits they can provide. To help navigate the choices that exist, it is recommended that airport senior managers, CISOs, and IT staff prioritize the countermeasures they wish to implement, assess the skills and availability of existing staff resources, and then select external service providers that can augment these internal capabilities to implement desired countermeasures.

As mentioned earlier, the overlap between service providers who can increase the likelihood of a cybersecurity attack and those that can decrease the likelihood will hopefully expand with time as more providers who operate at an airport are trained to help airports fight cybercrime by implementing the necessary countermeasures.

Passengers, Greeters, and Other Occupants

Previous sections have discussed the importance of training airport staff, tenants, and service providers to help protect the airport against cyberattack. Collectively, those groups are the smallest population at an airport. Passengers, greeters, and other occupants represent the largest groups of individuals at an airport. They should be considered when assessing vulnerabilities even though their direct access to and interaction with airport data and systems may be limited.

Passengers and greeters have access to publicly available Wi-Fi networks that most airports offer as a customer service. While these public networks are typically segregated from the airport's internal network, it may be possible for an attacker to gain access that affects passengers or airport operations or defaces the airport's image.

Passengers and greeters also have easy access to public portions of the airport where many secure devices such as HVAC controls, access control devices, CCTV cameras, and passenger screening devices exist. Passengers also have direct access to kiosks, vending machines, and other devices placed there for their use. Because passengers and greeters have a legitimate reason for being in these areas, it would be relatively easy for those looking to do harm to gain physical access to systems and devices in a manner that could increase the likelihood of a more serious attack.

There are numerous countermeasures that should be considered when securing data and systems exposed in public areas. Unlike with staff, tenants, and service providers, these countermeasures are limited to what can be done without active participation. Passengers and greeters are too numerous to effectively train and are not obliged to follow policies or procedures established by the airport. Regardless, the following measures can be taken to protect airport data and systems against cyberattacks from passengers and greeters:

- **Secure Wi-Fi** networks accessible to the public as previously discussed.
- **Disable or protect controls and ports on ICS** that are in public areas so that passengers and greeters cannot use them to gain a higher level of access.
- **Change default passwords** on devices that are accessible to the public. Often electronic devices, such as sign displays, kiosks, and screening devices have administrative or maintenance passwords that are set at the factory by default. These default credentials are often known to attackers. The access default credentials should be changed according to the airport's password policies upon installation and prior to the system being commissioned and put into use.

Considering passengers and greeters as potential attackers is important when designing a cybersecurity program that addresses all potential vulnerabilities. They should also be regarded as customers that may be affected by a cybersecurity attack. Treating this important population from both these perspectives can help an airport achieve the cybersecurity protection that it requires.

Private, Confidential, and Sensitive Information

All of these laws, regulations, and legal agreements require airports to protect personal and sensitive information. According to J. Razo of IBM (Razo 2012), a set of best practices for accomplishing this goal include the following:

- **Classify data** based on who has a need to know and the degree of harm (i.e., operational down time, financial loss, degraded safety) that may result from a breach or loss of the information. This should be done in coordination with other data stewards and senior management to ensure changes are consistent with organizational policy. Data classifications should include SSI, classified, airport use, and public. Additional distinctions that restrict data to certain groups of users within the airport may also be warranted. Financial, human resources, and airport security (other than SSI) information, for example, should perhaps be identified so that it can be restricted to certain user groups.
- **Develop organizational policy** for protecting information based on its relative sensitivity. Request that senior management approve of and enforce this policy. Provide guidance and instructions to managers and staff on adhering to, enforcing, and reporting infractions of this policy.
- **Appoint data stewards** to perform the following tasks:
  - Discover and inventory sensitive data.
  - Define additional discretionary security controls.
  - Periodically reevaluate the classification and protection measures in place.
  - Comply with laws, regulations, and best practices with regard to the data.
- **Introduce access monitoring software** to understand who is accessing information. This requires real-time analysis of system, application, and network logs to alert when unusual access behavior/pattern is detected.
- **Establish a process to remediate breaches** or leaks of information.
- **Periodically educate individuals** on how they need to secure sensitive information. This training can be part of the annual certification program. It is useful to highlight changes to both internal and external policies. Training should be prioritized for individuals who handle the most sensitive information.
- **Identify where information is stored** and implement additional protective measures if sensitive information is stored in zones outside the direct control of the airport. This should be accomplished as a part of the overall inventory of data and systems that may be vulnerable to cyber threat, as discussed earlier.

Working with personal, confidential, and sensitive information is a necessity in the modern workplace and at most airports. It is critical to identify the degree of sensitivity of the various types of data and the appropriate countermeasures to put into place.

CHAPTER 5

Developing a Cybersecurity Program

Chapter 4 covered how to identify cyber threats, assess their likelihood and impact, and implement countermeasures that provide protection. This chapter discusses how these activities can be supported and sustained by a comprehensive cybersecurity program. Over three-fourths of the organizations interviewed [32 of 41 (78%) respondents who answered the question] indicated that their organization has a cybersecurity program in place. Only half [19 of 39 (49%) respondents who answered the question], however, felt that the program provided adequate protection. The objective of this chapter is to help airports that do not have a cybersecurity program establish one, help those that do have a cybersecurity program improve its effectiveness, and, ultimately, help all airports sustain cybersecurity programs in a manner that is based on industry best practices. The key components of a cybersecurity program include the following:

- **Governance** encompassing laws, regulations, policies, standards, specifications, and procedures.
- **Training** to ensure that senior executives, managers, staff, tenants, consultants, and others understand the importance of cybersecurity and their role in protecting airport data and systems from attack.
- **Resources**, including the following:
  - **Staff** roles, responsibilities, and skills that are required to support a successful cybersecurity program.
  - **Funding** required to support a cybersecurity program and potential sources of funding to consider.
  - **External support** that can be tapped to help establish and sustain a cybersecurity program.
- **Ongoing activities** to maintain and continuously improve the effectiveness of a cybersecurity program.
- **Risks** of implementing a cybersecurity program and how to mitigate them.

These topics are intended to break the various aspects of an effective cybersecurity program into manageable components. Each topic is described in more detail in the sections that follow.

Information for IT managers and senior managers on the importance of, and how to approach, establishing and sustaining a cybersecurity program founded on best practices is provided in the multimedia material.

Cybersecurity Governance

Cybersecurity governance refers to how a cybersecurity program is controlled by the people entrusted to do so. Governance originates from a strategic perspective, but it guides and influences

the daily activities of these individuals as well as all stakeholders. Characteristics of governance include the following (Bodeau et al. 2010):

- How well the cybersecurity program is aligned with the overall risk management approach of the airport
- How pervasively and uniformly cybersecurity policy and measures have been implemented throughout the airport organization
- What level of support senior management provides
- How agile the program is to adapt to threats, countermeasures, and organizational change

Cybersecurity governance encompasses the legal requirements and regulations by which the airport must abide, policies that require standards and procedures to be followed, processes to ensure that data and software meet the airport's criteria, and contract and procurement mechanisms to obtain the proper external support. Collectively these elements allow an airport's cybersecurity program to be carried out in a consistent manner that is aligned with the overall organizational objectives. They also help managers make informed decisions about the priority of and the investment in specific countermeasures. The sections that follow discuss these elements of cybersecurity governance in more detail.

Legal Requirements and Regulation

There are numerous laws, regulations, and legal agreements to which airports are subject that should be addressed by a cybersecurity program. For each, senior management must determine whether the law or regulation is applicable to their organization and, if so, how they are going to enforce it. Following are some of the primary federal laws and regulations that airports should consider:

- **49 CFR 1520** defines how SSI is to be protected. SSI is information obtained or developed as security activities are conducted (49 CFR 1520.5). This encompasses information on security plans, directives, circulars, performance specifications, security measures, screening information, and training materials. Such information must be labeled as SSI (49 CFR 1520.13) and handled in a specific way (49 CFR 1520.19). Many airports have implemented SSI policies that communicate these requirements to their staff and consultants. Often these policies require individuals who have a legitimate need to access SSI to sign a form that acknowledges their willingness to adhere to this regulation. The CISO should ensure that employees and consultants are aware of the airport's policy and are periodically reminded of their responsibilities.
- The **Health Insurance Portability and Accountability Act** provides regulations on the management of health information of individuals. This act pertains principally to health care providers and insurers, although it also applies indirectly to employers, such as airports, who provide health care insurance and retain personally identifiable information (PII) on employees.
- The **Electronic Communications Privacy Act of 1986** prohibits unauthorized electronic eavesdropping (Fischer 2013). While there has been some debate as to whether this law encompasses emails temporarily saved on servers while in transit, airports may want to document their access to emails sent to or received by employees as part of their employment policy.
- The **Computer Fraud and Abuse Act** regulates abuse of "protected" computers, which include computers used in or affecting interstate or foreign commerce or communication. This act covers actions such as unauthorized access of or knowingly damaging such computers. Accordingly, airports are given legal protections against cyberattackers that extend beyond most organizations.
- The **Fair Credit Reporting Act** provides regulations for employers who use credit information for hiring, as well as businesses which provide data to credit rating agencies. This applies to the hiring and employment practices at airports that take these factors into consideration.

While the foregoing laws and regulations are pertinent to airports, there are a number of additional requirements placed on federal agencies. These are listed below as a reference. Airports may wish to consider some of these when defining their policies and procedures (Fischer 2013):

- The **Federal Information Security Management Act of 2002** clarified the NIST's role and strengthened its cybersecurity responsibilities, established a central federal incident center, and made the Office of Management and Budget (OMB) responsible for promulgating federal cybersecurity standards.
- **Executive Order 13636, Improving Critical Infrastructure Cybersecurity**, expanded an existing program for information sharing and collaboration between the government and the private sector, established a process for identifying and prioritizing the protection of critical infrastructure, tasked the NIST to lead in developing a framework of cybersecurity standards and best practices for protecting critical infrastructure, and required regulatory agencies to determine the adequacy of current requirements and their authority to establish requirements to address the risks. Many aspects of this order highlight the relevance of cybersecurity to critical infrastructure, of which airports are a vital component.
- **National Security Presidential Directive 51** and **Homeland Security Presidential Directive 20** established a National Continuity Policy to ensure the essential executive-level government functions are sustained in the event of a catastrophic emergency. The Federal Continuity Directive developed by the DHS provides operational guidance to support this policy. Portions of this guidance highlight the importance of collaboration and planning activities with local government that manages critical infrastructure such as airports.
- The **Clinger-Cohen Act of 1996** made agency heads responsible for ensuring the adequacy of information security policies and procedures, established the CIO position in federal agencies, and gave the Secretary of Commerce authority to mandate federal cybersecurity standards, a responsibility later shifted to the OMB as described previously.
- The **E-Government Act of 2002** serves as the primary legislative vehicle to guide federal IT initiatives to make information and services available online. It includes a number of cybersecurity requirements that may be relevant to airports.

Laws and regulations that are relevant to cybersecurity may also be imposed at the state, county, or municipal level. Despite the relatively new federal legislation described in the previous paragraphs, some feel that the federal government is currently grid locked in bi-partisan disputes, which will require states to become more active, especially in the wake of increasing retail and financial cyberattacks. States including Massachusetts and California are leading the way, and others are likely to follow (Camhi 2014). This trend is relevant to airports as many are directly managed by state, county, and municipal government agencies.

Individuals leading cybersecurity programs at airports should research the applicable laws by identifying the CIO or CISO of their parent organization and of the jurisdiction they are within. Local or regional FBI agents assigned to an airport as well as cybercrime units within local law enforcement offices can also help identify relevant rules and regulations for airports.

Standards and Guidelines

Numerous standards and guidelines support cybersecurity. Some of the key ones that airports should consider as a part of their cybersecurity programs are described in the following list. Unlike some of the laws and regulations previously identified, airports are not required to follow the standards and guidelines listed here. This is perhaps why relatively few [9 of 24 (38%) respondents who answered the question] reported using a national cybersecurity standard. As mentioned earlier, there are also few, if any, standards for ICS security at airports. Nevertheless, the research conducted, trends identified in other industries, and discussions with airport IT

professionals suggest that the following standards and guidelines are best practices and should be considered as a part of a prudent airport cybersecurity program.

- **Framework for Improving Critical Infrastructure Cybersecurity** was developed by the NIST in response to Executive Order 13636, which called for the creation of a cybersecurity framework to protect our nation's critical infrastructure. This framework provides a high-level structure for approaching cybersecurity at a national level. The NIST, working in conjunction with the DHS, developed and is promoting the application of these standards within governmental agencies and the private sector. In developing these standards, the NIST looked at the existing body of standards, regulations, and guidelines. For example, the international community had already developed the ISO 27000 series of standards. In addition, the NIST requested input from industry, academia, and government to create the final framework that was published February 2014 as Version 1.0. The result is a framework that delineates five high-level activities. These high-level activities establish the basis of the cybersecurity approach recommended previously in this document.
- **Information Security Management Systems requirements (ISO/IEC 27000:2013)** is a broad set of standards that define requirements for establishing, implementing, maintaining, and continuously improving an information security management system. These requirements are referenced extensively within the NIST Framework described previously. The ISO 27000 series of standards includes requirements for the assessment and treatment of information security risks as tailored to the specific organization. Complying with the ISO/IEC 27000:2013 information security management standards represents one approach to meeting the NIST Cybersecurity Framework. ISO details specific methods and processes that can be mapped directly to the five phases in the NIST framework outline and offers approaches for organizations of any size and budget.
- ***An Introduction to Computer Security: The NIST Handbook*** (**NIST 800-12**; Guttman and Roback 1995) provides a broad overview of computer security and control areas. It also emphasizes the importance of the security controls and ways to implement them. Initially, this document was aimed at the federal government although most recommendations in it can and are being applied within non-federal agencies and other organizations as well. Although this document was originally published in the late 1990s, it remains an excellent source of training for personnel seeking to become acquainted with computer security best practices.
- ***Security and Privacy Controls for Federal Information Systems and Organizations*** (**NIST 800-53**) provides a detailed and prioritized list of countermeasures. The document was developed by an interagency working group with members from civil, defense, and intelligence agencies. It has been revised several times to keep up with the rapidly evolving landscape of threats and the countermeasures available to confront them. The catalog is an excellent list of threats for airports to consider and is provided as a reference in Appendix A.
- ***Guide to Industrial Control Systems Security*** (**NIST 800-82**; Stouffer et al. 2013) provides guidance on the threats against and countermeasures available to help protect ICS from cyberattack. The document describes typical ICS topologies and where vulnerabilities may exist. It acknowledges the unique performance, reliability, and safety characteristics of these systems that must be considered as the impact of threats are assessed and countermeasures are implemented.
- **North American Electric Reliability Corporation**'s critical infrastructure protection plan encompasses nine standards and 45 requirements designed to protect the nation's power system from cyber, physical, and other types of attack. Many of the requirements can support protection of airport data and systems.
- **PCI DSS** are intended to provide guidance and certification criteria for organizations that process credit cards; however, the applicability of these standards is far more encompassing. This standard is described in detail in the following section.

Despite the relevance of these standards, some respondents [4 of 24 (12%) who responded to the question] replied that the available standards were not appropriate for their environment. A 2014 Verizon study found that this is particularly true among smaller organizations that do not have the depth of knowledge or specialization in cybersecurity (Verizon 2014).

Although cybersecurity standards have not been fully embraced by airports, greater awareness of them through this and other publications may increase adoption rates. This trend will likely continue as new cybersecurity standards and guidelines emerge with a greater focus on aviation-specific cybersecurity needs. Individuals responsible for cybersecurity programs at airports should consider standards an effective resource for developing their policies and procedures.

Payment Card Industry Data Security Standards

The PCI DSS have been established by major credit card companies, including American Express, Discover Financial Services, JCB International, MasterCard, Visa Europe, and Visa Inc. The PCI Security Standards Council was established in 2004 and funded, in part, by these firms, as well as the fees generated through training, assessment, and other services. Their motive was to counter the growing breach of credit card information that can occur at the POS, in transit, or in a database.

To elevate the awareness and level of protection credit card processors have in place, the PCI Security Standards Council published the PCI DSS, which is now in Version 3.0. According to a 2014 study, "Version 3.0 [of the] PCI DSS is more mature than ever, and covers a broad base of technologies and processes such as encryption, access control, and vulnerability scanning" (Verizon 2014).

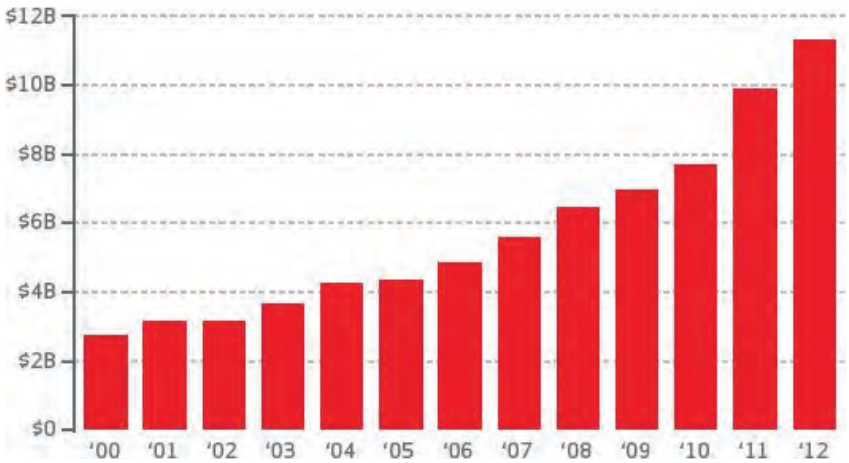
The PCI DSS represent a comprehensive set of practices, assessment methodologies, and certification guidelines for protecting credit card information, issuers and processors, and, ultimately, consumers. The standards encompass much more than payment processing and include aspects of employee training and awareness as well as network and IT operational planning and practices. PCI DSS furthermore provides a solid foundation for the protection of PII, which is now subject to regulation in 47 states. The first such law was passed in 2002 in the state of California as SB 1386 and became effective in 2003. Other states have followed with their own variants. Of interest to airports is that SB 1386 relates to the protection of the information of California residents wherever that data resides. So a breach of PII in one state could require notification of residents in many other states.

For these reasons, several airport CIOs and CISOs feel that the PCI DSS are good practice regardless of the level of credit card processing their airport does. It is also a requirement that credit card companies may place on airports that process credit cards to collect parking, employee badge, and other fees. Airport tenants may also transmit credit card information via the airport's network, transferring some of the responsibility for protecting this information to the airport.

Accordingly, most respondents [24 of 31 (77%)] claim their organizations comply with PCI DSS. This is, however, lower than the 84% found across other industries in a Verizon survey of 4,000 companies (Verizon 2014). Note that many companies report only a Level 1, or basic, compliance. Those that comply at a higher level, according to the Verizon survey, are statistically less likely to experience a breach.

General Compliance

Since the PCI DSS were introduced 10 years ago, a significant number of organizations have implemented them or become compliant (Verizon 2014). Despite this growth, many organizations have not yet achieved the basic level of compliance. Those organizations that are breached



Source: HSN Consultants, Inc. (2013).

Figure 5. Global credit card losses.

tend to be less compliant. This problem continues to grow as evidenced in the growing amount of credit card fraud losses as summarized in Figure 5 (HSN Consultants, Inc. 2013). Recent, heavily publicized breaches of credit card information at national retailers, including Target and Home Depot, further accentuate the problem (Depner 2014). Industry analysts expect this trend to continue (McAfee 2014).

Applicability to Airports

To be PCI DSS compliant, an organization must meet the 12 requirements in the following list, which encompass business processes and training as well as securing network, software, and devices (PCI Security Standards Council 2013). Many of these countermeasures have been discussed in other sections of this document. They are repeated here as they are specifically called out as a requirement of compliance with PCI DSS.

- **Install and maintain firewall(s) to protect cardholder data.** It is recommended that an organization's network infrastructure be segmented to isolate the cardholder data environment (CDE) from other networks. In an airport, there may be multiple CDEs that are kept independent of each other to prevent the breach of one network in a manner that impacts the integrity of another. For example, individual airline tenants may have isolated networks or be separate from the network provided for retail operations. Properly configured firewalls can isolate CDE networks from each other as well as the larger open, public network that should be considered insecure. Some airports have achieved this level of isolation by outsourcing activities that require credit card processing, such as the collection of parking fees. Some feel that the loss of revenue to these third party vendors is offset by the reduced risk level they achieve.
- **Do not use vendor-supplied default passwords and other security parameters.** Vendors ship systems with default settings and administrative passwords. These default passwords are often commonly known and therefore a vector for breach. In fact, there is a public website listing default passwords for 485 vendors with approximately 2,000 passwords (CIRT.net 2014). The selection of settings and choice of passwords should be part of an overall configuration management and security plan.
- **Protect cardholder data stored in databases.** Protection methods such as encryption, truncation, masking, and hashing are critical to protecting cardholder data or other sensitive data. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other

effective methods of protecting stored data should also be considered as potential risk mitigation opportunities.

- **Restrict physical access to vital data and systems.** Airports are very familiar with the need to physically restrict access to certain areas and systems. This requirement applies to data and systems that handle, route, store, process, or enter critical information. Visitors including non-badged contractors, vendors, customer service representatives, and repair personnel must be escorted by an authorized airport staff member.
- **Use strong encryption and key management** for vital data in transit across public networks. The use of VPN, the secure hypertext transfer protocol, and SSL encryption has become industry standard for the transmission of sensitive or confidential data. Maintaining a robust key management system or automating with one-time session-based keys reduces the vulnerability to man-in-the-middle attacks or sniffing.
- **Protect all systems against malware and regularly update antivirus software.** As new malware is created, anti-malware vendors create new signatures and procedures to mitigate the potential damage. The rate at which new malware is created, however, continues to grow and zero day attacks will continue to be discovered. Therefore, staying current with the real-time intrusion detection and prevention systems is now a standard requirement. Patching applications and operating systems is also an important measure. This can be a challenge when legacy applications cannot keep up with the rapid changes in newer systems. Segmentation, isolation, and monitoring of such legacy systems are the next line of defense for these cases where security updates are not available or anti-malware solutions are not offered.
- **Develop and maintain secure systems and applications.** New or expanded systems should be designed to be as isolated as possible without impairing any required functionality. This includes not connecting other databases, systems, or networks to the CDE. Any new application should follow secure development processes and testing to avoid common vulnerabilities such as buffer overflow, cross-site scripting, or structured query language (SQL) injection.
- **Restrict access to cardholder data based upon a business need to know.** Segregate access to critical infrastructure with strong authentication and only provide credentials to a limited number of the staff members that have a valid need to know. Use distinct and unique credentials for the sensitive data system components to prevent escalation of privileges that can impact more critical systems. For the most sensitive systems, two-factor authentication is recommended and in some instances required.
- **Identify and authenticate access to system components.** Unique access credentials for all users are required. Authentication methods should curtail frequent access attempts with incorrect credentials. If such frequent attempts occur, notification or alerts should be sent to system administrators who may be able to prevent intruders attempting to gain access.
- **Monitor and log all access to critical systems.** Logs for network access, critical systems access, and system change are critical for monitoring, detecting, and minimizing the impact of a cyberattack. These logs must be retained for at least 6 to 12 months in order to analyze and trace an event when something does go wrong.
- **Regularly test security systems and processes.** Malicious entities and security researchers are constantly discovering new vulnerabilities. The procedures, systems, controls, and hardware and software configurations must be put on a regular test schedule to ensure adequate protection. The period for testing will vary by component as some vectors such as mobile and wireless are evolving more rapidly than others.
- **Maintain a policy that addresses information security for all personnel.** A strong security policy demonstrates to all personnel the importance that the airport places on cybersecurity. Personnel include vendors, contractors, and external personnel that regularly work at the airport. Regular training covers the awareness portion of PCI DSS. The organization is best protected when everyone who may touch cardholder data understands the importance of managing that data. Extending this to the critical data that is used for the safe operation of the

airport provides the best risk posture possible. PCI training can be offered to airport personnel, tenants, and consultants.

While PCI DSS compliance is a requirement for airports that process credit card information, many are implementing some or all of the preceding countermeasures as a matter of good practice. Note that, while PCI DSS compliance may be a requirement or good practice, it has "never been a catchall solution" (Depner 2014). It is "more like an acknowledgment that you're not incompetent" (Depner 2014) and is a good set of countermeasures that airports should consider.

To determine the scope of PCI implementation best suited to an individual airport, it is recommended for stakeholders to complete a questionnaire to discover all of the systems, networks, devices, and processes involved in the entry, storage, transmission, monitoring, and interactions with credit card data. Once the scope is determined, another questionnaire can be completed to determine the airport's readiness and what steps are required to move it toward compliance.

Policies

There are numerous policies that should be considered and, as appropriate, adopted by an airport as a part of its cybersecurity program. These policies will help ensure that the airport remains in compliance with the laws and regulations as well as the applicable standards and guidelines previously described. They will also help ensure that staff, tenants, and consultants are aware of and embrace the countermeasures that are germane to them. Following are some of the primary policies that airports and other organizations have adopted in support of cybersecurity:

- **Acceptable use** of data and systems should be established by policy. All staff, tenants, consultants, and other stakeholders who have access to airport data and systems should be required to use these resources in a manner deemed acceptable by senior management. An acceptable-use policy should cover what types of data and systems can be used for specific types of work activities by specific individuals based on the role they play, how access credentials to these resources should be protected, and how to report intentional or mistaken misuse.
- **SSI** should be defined and handled as called for in 49 CFR 1520. While this regulation documents national policy, it is general and does not specifically identify the information that may be considered SSI at a specific airport. A recommended best practice, which some airports have followed, is to develop a policy document that references 49 CFR 1520 but extends it to list the specific information found at the airport that is SSI. This policy document should name specific security systems and procedures found at that airport, using terms familiar to managers and staff. The policy should also define or, at least, reference procedures on how SSI is to be handled, provide instructions on how to request access to SSI, name who at the airport has authority to grant this access, and explain what to do if SSI is inadvertently released. This policy should be distributed to any airport staff, tenants, or consultants that may come into contact with SSI. It is important that these individuals understand that this policy is a critical job responsibility and it is also critical that they receive the necessary training on how to identify, handle, and dispose of SSI.
- **Private information** should be defined and protected as a matter of policy. This will help the airport remain compliant with laws that protect personal health care records, credit card information, and other forms of PII. In some cases, airport staff members may have a legitimate need for this data (e.g., to support employee benefit programs and to charge employees for badge processing and other fees). In these situations, authorized employees must be aware of their rights and responsibilities for handling this information. Others, perhaps as a part of the cybersecurity training, should be aware of what is considered private information, what the airport's policy is with regard to the handling of private information, and how they should report any deviations from this policy. This awareness will not only help enforce the airport's privacy

policies but will also provide some assurance to all employees that their private information is handled in a compliant and conscientious manner.

Recommended policies for airports to consider to support cybersecurity best practices are provided for both IT managers and senior managers in the multimedia material.

- **Software and data assurance** should be required of all staff and consultants involved with developing software or digital data. This assurance should encompass system specifications that will reduce vulnerabilities in software applications and systems, data specifications that are relevant to cybersecurity, testing procedures for both software and data to ensure they meet these specifications, and a process to certify that these requirements have been met. While software assurance policies are typically focused on IT vendors, they should also be extended to vendors of ICS. Similarly, data assurance policies should be extended beyond the IT developers of databases, web services, and other data sources to include consultants and contractors that develop any form of digital deliverable for the airport.
- **Training** should be required of all staff as a condition of employment. Training should also be required of contractors, consultants, and tenants as a condition of their contracts and agreements with the airport. This training should be administered periodically, such as on an annual basis. While the overall message of this training will not change much, the specifics of what to look for and how to react may change as the nature of threats evolve. It is also important that staff, contractors, consultants, and tenants be regularly reminded of their responsibilities. This training is very similar to, and in fact can be administered along with, the annual security training that airports require of individuals who have been issued an airport security badge.
- **Communications** about threats, vulnerabilities, and attacks should be controlled by policy. The goal should be to foster quick and efficient communications with appropriate parties but in a manner that does not compromise sensitive information or the airport's reputation. The policy should also establish how airport managers and staff should react when certain information is received. This should be established and communicated to the appropriate stakeholders well in advance of an attack occurring so that they can respond in an efficient manner without divulging or reacting to inappropriate information.

The preceding policies are recommended, but each airport's management should determine their applicability and how they should be adopted within their individual organization. This requires input from technical staff and perhaps representative staff, vendors, and consultants who will be affected by these policies. These policies should also be consistent with and complementary to other policies the airport or its parent organization may have in place. The development of these policies can be led by the individual(s) responsible for cybersecurity, but it is ultimately the responsibility of senior management to endorse and enforce the policies that are developed.

Contracts and Procurement Considerations

Most of the systems and much of the information used by airports are provided by external service providers or other organizations. It is the airport's responsibility to ensure that its cybersecurity requirements are met before these data and systems resources are installed and used. To achieve this goal, it is prudent that cybersecurity requirements be incorporated as early as

possible into the procurement process so that qualified service providers responding to the airport's solicitations are fully aware of the requirements they must meet.

Simply selecting a qualified provider is not enough. To effectively integrate cybersecurity requirements into the procurement process, IT and facility managers should work with procurement managers to ensure that their functional, technical, and security-related requirements are all properly incorporated into system and data procurement solicitations and the contracts that result. Developing such specifications may require the use of external literature, agency, and consultant resources. Selected providers should also be asked to review and recommend security measures that are best practice for their particular product for the airport to consider. Once mutually agreed upon, all cybersecurity requirements should be documented within the provider's scope of work and checked before final payment is made. These precautions apply to products and services that will ultimately reside on-site at the airport as well as cloud-based services that airports are increasingly using.

Some airports [9 of 32 (28%) respondents who answered the question] are already following this best practice. A greater number [15 of 32 (47%) who responded to the question] factor cybersecurity needs into their procurement process but do not explicitly incorporate requirements. As cybersecurity awareness increases among senior management, it is likely that more airports will adopt these practices, the most critical of which are as follows:

- **Airport policy** should establish rules governing data, software, system, and device procurement requirements and procedures. This should be at a general level, so as to be relevant to all airport procurements that involve data and systems (Information Security Standards 2014).
- **Procurement, IT, and facility managers must collaborate** to develop functional, technical, and security-related requirements that are specific to each data resource, system, or device that is procured. In some cases, assistance from an external technical expert who is not allowed to bid on the procurement and has no financial interest in any of the bidders may be required to assist.
- **Commercial-off-the-Shelf (COTS)** solutions that have had vulnerability tests and have been operating in similar, ideally airport, environments should be preferred over custom solutions. Where COTS solutions cannot adequately meet airport functional and/or technical requirements, vendors who propose custom solutions must provide assurance that the solutions have been implemented using cybersecurity best practices (Information Security Standards 2014).
- **Secure outsourced or custom development** by requiring developers to protect code from the embedded malware that may ultimately be introduced into the airport environment (Information Security Standards 2014).
- **Secure data provided to consultants and developers** by requiring them to adhere to the airport's acceptable-use policies. Consultants or developers that are required to handle SSI should acknowledge that they will do so in accordance with the airport's SSI policy and ultimately 49 CFR 1520. This should apply to consultants before (i.e., during procurement with provided SSI), during (i.e., while under contract), and after (i.e., after the work has been completed and before SSI is returned or properly disposed) the contract.
- **On-site or remote installation** of data, software, or systems should be carried out in accordance with the airport's IT access and/or physical security requirements. This may require badging of consultants and developers, signing of access and acceptable-use policies, and possibly escorts into secure areas of the airport. It is important that these requirements be clearly stated during the procurement process so that associated costs and time durations are factored into the bids that are received.
- **Unused code or services should be disabled or removed** by the developer prior to installation. This limits the exposure of the system due to code or services that are providing no value to the airport. The developer should indicate in the documentation which portions of their

code and/or services have been disabled as a part of their configuration management process (adapted from ICS-CERT).

- **Documentation should be delivered** that details all applications, utilities, system services, scripts, configuration files, databases, other software required, and the appropriate configurations. This should include documentation on revisions and/or patches for each of the computer systems associated with the control system. This documentation should list all ports and services required for normal operation as well as any necessary for emergency operation. This documentation should be referenced in the inventory of airport systems (adapted from ICS-CERT).
- **Commissioning or certification** of the data or systems that have been procured should include checks by airport staff or consultants that are independent from the vendor that ensure proper cybersecurity countermeasures have been put into place and that all associated airport policies and procedures have been followed.
- **A warranty should be required** that ensures the vendor or developer will provide updates and patches to their information or system for a period of time specified by the airport. The airport should consider requiring, as a part of this warranty, the vendor to assess and mitigate any vulnerabilities or impacts of successful attacks against their systems. It should be noted that these types of warranty requirements, especially those extending significantly into the future, create risk for vendors that must be compensated. An adequate balance between the costs and benefits should be considered by airport cybersecurity and risk management personnel (adapted from ICS-CERT).

Although these requirements can add time and therefore cost to the procurement process, they will help ensure that the airport's cybersecurity requirements are adequately addressed as new systems are installed. Although burdensome, this cost is significantly lower than the cost of vendor change orders and, ultimately, the cost of responding to and recovery from a cyberattack due to vulnerabilities by a newly installed system.

Software and Information Security Assurance

The software and data that airports acquire from consultants, vendors, and others may introduce vulnerabilities that should be addressed before the software or data is installed and used at the airport. In some cases, the data and systems are developed in-house by airport staff. These employees should follow the same procedures required of external providers to ensure the airport that the software and data they provide is secure. Following are guidelines on how they can provide this assurance and the role airport cybersecurity professionals should play in enforcing them.

Software Assurance

Software assurance is "the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner" (Committee on National Security Systems 2010). The objective of software assurance is to ensure that "the processes, procedures, and products used to produce and sustain the software conform to all requirements and standards" (Mercedes and Winograd 2008). To support cybersecurity objectives, software must be ensured to be free of vulnerabilities to the extent possible, not introduce vulnerabilities to other systems, and continue to operate as intended if anticipated attacks occur.

These goals can be compromised due to design, development, or deployment mistakes; intentional vulnerabilities introduced by vendors, users, administrators, or others who can gain access; and technology changes that can introduce threats not anticipated by developers (McGraw 2006). Some of the threats that can impact software include command injections, SQL

injections, vulnerable operating system interfaces, buffer overruns, leaks of memory not freed when software is done with them, memory pointer errors, format string attacks, and integer overflow or truncation errors (Software Assurance Marketplace 2014). In addition, web-based software also can be exposed to cross-site scripting, uniform resource locator (URL) redirection, and credential exposure. While there are many threats, the top 25 software vulnerabilities have been ranked by the SANS Institute working in conjunction with the MITRE Corporation (Christey 2011). This list can provide an important reference that can be used as a checklist for software assurance programs.

However, the complexities of developing, implementing, and maintaining software with the assurance of not being vulnerable to cybersecurity threats do not need to fall on airport managers or staff. The technical skills and familiarity with the software needed to combat these threats necessitate that developers and installers provide these assurances. These individuals will typically be employed by vendors or third party installers, although in some cases, airport staff may develop custom software in-house as well. The individual(s) responsible for cybersecurity at an airport must require developers and installers of software that is used at the airport, regardless of where they are employed, to perform the following assurances:

- **Build security into the software development life cycle** at each phase. This starts with design, as flaws at this stage account for 50% of security problems (McGraw 2006). The languages, third party components, and even the development environment should be adequately secured (MITRE Corporation 2014a).
- **Test software and systems** for known vulnerabilities prior to deploying them. There are many tools and processes that can be used to test software for security vulnerabilities; some of these are free (Software Assurance Marketplace 2014).
- **Protect application credentials** by not hard coding password and security tokens in code that can be accessed by users or outsiders. Credentials, as well as any data that can be considered sensitive or confidential, should also be encrypted as they are transferred between servers and end-point systems or client devices.

These requirements should be enforced by airport policy and incorporated into contracts with vendors and third party installers. Airports may wish to require a written certification of these assurances from vendors and installers. Warranties that ensure software is free of vulnerabilities for a defined period of time may also be desired. These measures will come at a cost that senior managers must consider in relation to the level of protection they desire.

The software assurance responsibilities of airport managers and staff do not end with the enforcement of policy on vendors, installers, and in-house developers. The individuals responsible for cybersecurity should also perform the following:

- **Install software patches and updates** promptly upon their release, ideally by automated means if possible.
- **Report bugs and vulnerabilities** that can be attributed to the software to the vendor. Vendor points of contact should be included and maintained as part of the system inventory described earlier.
- **Restrict software installation privileges to IT personnel** who are knowledgeable about which software sources can be trusted or not. If airports allow employees to bring their own devices, then policy and procedures that require and enable the owners of these devices to be vigilant in this regard should also be considered.

Some of the primary practices for ensuring software security are described above. There are many more resources to help airport cybersecurity professionals, developers, and installers ensure that the software conforms to an airport's security requirements. Several of these are listed on the DHS website (under Software Assurance Resources).

Information Assurance

As with software, information, or data, can introduce vulnerabilities that should be minimized or eliminated. For example, information that is SSI as defined by 49 CFR 1520 but that is not labeled as such increases the likelihood that such information will be leaked to those not authorized to view it—an issue that at least one large airport has experienced. Information, or data, should also be assured to have integrity (i.e., not have been altered), availability to those who need and are authorized to access it, and authenticity with its source known (Information Security Standards 2014).

As with software assurance, information assurance should start with defining the requirements that define the integrity, availability, and authenticity expected. These requirements should be documented in information security standards, data clauses of acceptable-use agreements, and non-disclosure statements. These standards or specifications should be enforced by airport policy and reflected in consultant contracts, tenant agreements, and employment conditions. They should cover the following key practices of information assurance, which are related to cybersecurity:

- **Legal requirements, regulations, and agreements** must be met. These include laws such as 49 CFR 1520 that protects SSI, the FAA's requirement for certificated airports to record operational data, and agreements with credit card companies to adhere to PCI standards.
- **Non-disclosure agreements** and **acceptable-use policies** should be established to ensure that data is used by authorized individuals with a legitimate need to know. These individuals must also be informed of the sensitivity of the data they possess and how to handle it. This includes providing the proper level of cyber and physical protection of data whether they are on-site at the airport or off-site in consultant and tenant offices.
- **Label** all data to indicate its contents, source, temporality (i.e., for what date ranges the data is valid), and sensitivity level.
- **Transmittal letters** should accompany data deliverables that assure that the data meets all applicable airport and legal requirements of that data.
- **Archive original copies** of data so they can be recovered in their original form if required.
- **Backup operational data** so that normal operations can be resumed quickly and efficiently if data is corrupted as a part of an attack.

Airports may also want to consider factors beyond cybersecurity when providing information assurance for data delivered to them as well.

These and other precautions may be considered by airports on a case-by-case basis to help protect the usability of data. While hardware, software, and network devices are essential elements of IT infrastructure, it is ultimately the data that is required by end users and must therefore be of the quality they require.

Resources Required

There is no minimum threshold of resources or investment that is required to establish and maintain a cybersecurity program.

Effective cybersecurity programs require an appropriate mix of internal and external resources in order to be effective. Internal resources include airport staff. Funding is also required to obtain external resources such as consultants, vendor services, training programs, software, and possibly hardware. This funding may come from airport operating funds and other sources and be incorporated into budgets of capital programs.

The level and mix of resources required will vary greatly based on the size of the airport, the propensity of management to use internal staff versus external consultants, existing staff skills available, availability of qualified consultants, and other factors. Using no external resources is

Each airport must determine the appropriate balance between risk mitigation and the opportunity cost of the resources they have.

not an advisable option as some of the skills and capabilities required are not needed 100% of the time and would be expensive for an airport to retain. Furthermore, there are low-cost or, in some cases, free external resources (e.g., ISACs) that can be tapped to maximize the cost-effectiveness of an airport cybersecurity program. Conversely, outsourcing all aspects of a cybersecurity program is not feasible because decisions, priorities, and funding decisions must be made by individuals who have a broad perspective of the airport's needs and who are ultimately going to be held accountable for a successful attack. Between these two extremes, however, there is a wide range of possibilities.

There is no minimum threshold of resources or investment that is required to establish and maintain a cybersecurity program. On one end of the spectrum, an airport can read freely available material to become aware, utilize free training and information sharing resources, install low-cost end-point protection, and remain vigilant. On the other end of the spectrum, an airport can spend significant funds on training, consultant, and other external resources. The senior management of each airport must, with the help of IT and consultant resources if available, determine the appropriate balance between risk mitigation and the opportunity cost of the staff and financial resources they have.

To support this decision, this section describes the types of resources that are required and the range of options that exist based on current industry practice. Trends are also noted as the demand and supply of cybersecurity resources is rapidly growing and evolving. Where possible, guidelines are offered to help senior managers decide on the appropriate level of investment in cybersecurity for their airport.

Staffing

Whether new staff are hired or existing staff are assigned new responsibilities, cybersecurity requires attention from airport managers and staff. Before the level of staff resources required can be determined, it is important to review the key roles that must be fulfilled, determine where they best fit within the organization, and assess the capabilities (i.e., skills, education, experience, and training) and capacity (i.e., availability or more likely the impact of not accomplishing some existing tasks) of available staff. The gap that remains between the capabilities required and the capacity available is a gap that needs to be filled. To do so may require augmenting the capabilities and capacity of existing staff with new hires and/or external resources.

Cybersecurity Roles

There are 12 primary organizational roles that must be fulfilled to support an effective cybersecurity program. Note that a role is not the same as a full-time equivalent (FTE). In some organizations, individuals will be assigned multiple cybersecurity roles, perhaps in addition to other airport duties. In other organizations, one or more individuals may fulfill a specific role. The 12 roles are as follows:

- **Senior management** must be aware of and remain informed about the threats their airport faces, the likelihood those threats may impact critical information or systems, and the cost that impact may have on safety, efficiency, revenue, and reputation. This requires awareness training and periodic briefings. It also requires support from IT and facility managers who can provide the details at the appropriate summary level to help senior managers make informed decisions. During budget decision cycles, senior managers should evaluate the organization's investment in cybersecurity using metrics against alternative investment options.
- **Chief information officers** are often entrusted with the security of an organization's data and systems. Some CIOs interviewed for this study felt that this responsibility may not be well placed since they also have a responsibility to provide a level of access to data and systems.

The objectives of providing access and reducing cybersecurity risk are often at odds. They recommend having a separate individual, such as a CISO, be responsible for cybersecurity and report to senior management or whoever within the airport is responsible for organizational risk, legal, or regulatory matters.

- **Chief information security officer** (or cybersecurity manager) is an increasingly common title within organizations including airports. Such individuals should be trained in cybersecurity principles and be prepared to carry out or manage the activities that are required. They must remain aware of the range of threats airports face and the options available to counter them. CISOs must identify, acquire, and lead the application of human and financial resources required to provide the level of protection desired by senior management. To accomplish this, CISOs should be prepared to identify and to the extent possible, quantify risks. They should be prepared to advise Senior Managers on matters of policy and collaborate with managers throughout the organization on the enforcement of that policy. They should be prepared to work with IT managers and staff to design and implement an enterprise approach to implementing countermeasures. CISOs should also establish and maintain relationships with external service providers and agencies that can help the airport periodically assess vulnerabilities, carry out day-to-day cybersecurity activities, and respond should an attack occur (NICE 2014).
- **Security managers** are entrusted with the physical security of the airport. This can encompass access control, monitoring CCTV cameras, and incident response. This function sometimes falls under Operations or other departments. Sometimes, their responsibilities are extended to include airport cybersecurity as well. Other times, physical aspects of security are handled by local law enforcement. Regardless of their responsibility over cybersecurity and their organizational affiliation, security managers should be aware of cybersecurity principles and the importance of controlling the physical access to airport data, systems, and network devices. They must also be aware of the SSI that they manage and how such information should be identified and protected.
- **Application managers** ensure that the business requirements of end users are addressed through software installed on local desktops, on servers, or in the cloud. They help enforce the airport's software assurance policy and work with vendors as new systems are selected, installed, and configured to ensure cybersecurity requirements are met.
- **IT infrastructure engineers** research, develop, and implement IT infrastructure components such as servers, network switches, and routers. They have input to the configuration of end-point systems. Infrastructure engineers should also record changes to the configuration of the airport's network. This continuously updated inventory serves an important purpose when assessing the likelihood and impact of an attack on the airport as well as when returning to normal configuration after an incident.
- **IT operations** staff oversee databases, storage devices, and other services that support business applications, end-point systems, and network infrastructure. Typically, operations staff work a help desk to provide airport staff and, in some cases consultants, with the IT support they require. With regard to cybersecurity, they monitor network logs looking for anomalous activity. They assist end users with troubleshooting and reporting issues that may be related to a cyberattack. Often, IT operations staff will be responsible for patching and upgrading systems and applications, which is an important countermeasure.
- **Facility managers** are often the ones to specify requirements for, oversee the implementation of, and monitor operations and maintenance of ICS at the airport. They should be aware that such systems face cybersecurity threats and should ensure, with the help of others, that effective countermeasures are put in place as these systems are selected, procured, and installed.
- **Procurement managers** ensure that qualified vendors are selected to provide the airport with the products and services required. They ensure that cybersecurity requirements including software and data assurance requirements, technical specifications, data use agreements, and

other cybersecurity measures are included in airport business solicitations and the resulting contracts that are awarded. They must work with IT and facility managers as these documents are developed to ensure that the proper technical requirements are properly reflected. The CISO should be made aware of procurement documents so that the proper requirements can be put into place before they are released.

- **Human resource managers** should be aware of the laws and regulations regarding personal information and should be prepared to protect that information as required.
- **Trainers** are required to promote cybersecurity awareness and conduct or administer training for airport staff, and perhaps consultants, tenants, and other stakeholders.
- **Users** of airport data and systems play an important role in protecting the organization against the many threats that exploit human behavior such as phishing attacks. Users should be periodically trained, remain vigilant to activities that may be related to an attack, and report suspected issues.

Some of the primary roles involved in supporting an airport cybersecurity program are highlighted in the multimedia material. Different types of users can select the role they play and view lessons, content, and resources that fit their needs.

Developing and maintaining a team of staff and consultants who can adequately fulfill the preceding roles can be challenging. Sometimes unqualified individuals may be offered a position and not be aware of the expectations they should fulfill or of training resources that exist. The following resource can help airport senior managers, human resource managers, CIOs, and procurement managers identify and train individuals qualified to fulfill the preceding roles.

- The Interactive National Cybersecurity Workforce Framework provides lists of tasks and knowledge, skills, and abilities (KSAs) required of cybersecurity professionals, including CISOs. These have been summarized in the preceding list, but airport managers looking to hire or train cybersecurity staff members can consult this interactive document to ensure that they develop an adequately prepared cybersecurity workforce (NICE 2014).

The Interactive National Cybersecurity Workforce Framework has been included as a library resource for senior managers and IT managers in the multimedia material. It can also be found at http://niccs.us-cert.gov/training/tc/framework. An interactive PDF version can be downloaded from the National Initiative for Cybersecurity Education (NICE) website http://csrc.nist.gov/nice/framework/. Page 146 of the PDF file describes the tasks and KSAs for a CISO.

Staffing Levels Required

The previously described roles each bear some of the responsibility for protecting an airport against cybersecurity threats. The activities that must be carried out to fulfill that responsibility include training, monitoring logs, procuring services, supporting user needs, and following procedures. Should a successful attack occur, response and recovery activities are also required. The time required to fulfill those responsibilities can vary widely based on the role(s) fulfilled

by each individual, the size of the airport, and the degree of risk protection senior management decides to implement.

To evaluate the staffing needs of a cybersecurity program it is prudent to assume that absent of any cybersecurity responsibilities, airport staff members are fully engaged and productive. In other words, no staff members have extra time on their hands to complete cybersecurity activities without there being some impact on the airport. This assumption establishes a baseline from which the staffing needs of a cybersecurity program can be assessed.

Table 2 summarizes the range of staffing levels required to support an effective cybersecurity program at an airport. The figures are expressed as FTEs, which means a fully employed individual less paid vacation, sick, and other paid-but-not-work-related time. Typically, an FTE equates to 1,700–2,000 labor hours per year depending on the working hours, benefits, and paid programs offered. Using this approach, the lower end of the staffing requirement for a cybersecurity program is 0.3 FTE. This is spread across multiple roles and is not enough to justify a new hire. At the other end of the range, airports may require as many as 2.65 FTEs to support a cybersecurity program, thereby justifying two or three new positions. It should be noted that for several roles there is a minimal impact, which is too small to factor into such staff planning decisions and should be considered a cost of doing business.

As indicated in Table 2, several of the roles associated with cybersecurity can be outsourced. In fact, just over half [16 of 30 (53%)] of the organizations surveyed responded that they outsource some of their cybersecurity roles. A greater number [21 of 29 (72%) respondents to the question] indicated outsourcing vulnerability assessments, which makes sense because of the highly specialized skills that are required and because this activity is not continuously required. Such outsourcing effectively lowers the investment of staff time required. Not all roles however are prone to outsourcing. Senior managers, facility managers, procurement managers, human resource managers, and users all play a role in cybersecurity, but they are fundamentally a part of an airport's staff and cannot simply be outsourced to support the needs of a cybersecurity program.

While this section is not intended to present a rigorous staff planning or justification analysis, it will hopefully provide some guidance for planning the proper cybersecurity resources. It is clear that cybersecurity cannot be effectively applied without staff participation. It is also clear that new departments and legions of new hires are not required, especially given the growing potential to rely on outsource resources to support many of an airport's cybersecurity needs.

Table 2. Staffing requirements for a cybersecurity program.

	New FTE	Outsourcing
Senior Management	Minimal	
Chief Information Officer	.1-.25	Possible
Chief Information Security Officer	.1-1	Possible
Airport Security	Minimal	Possible
Application Managers	0-0.15	Possible
IT Infrastructure Engineers	0-0.25	Possible
IT Operations	0.05-0.5	Possible
Facility Managers	Minimal	
Procurement Managers	Minimal	
Human Resource Managers	Minimal	
Trainers	0.05-0.5	Possible
Users	Minimal	
Total	0.3-2.65	

Source: Interviews with airport CIOs and IT managers.

Organizational Structure of Cybersecurity

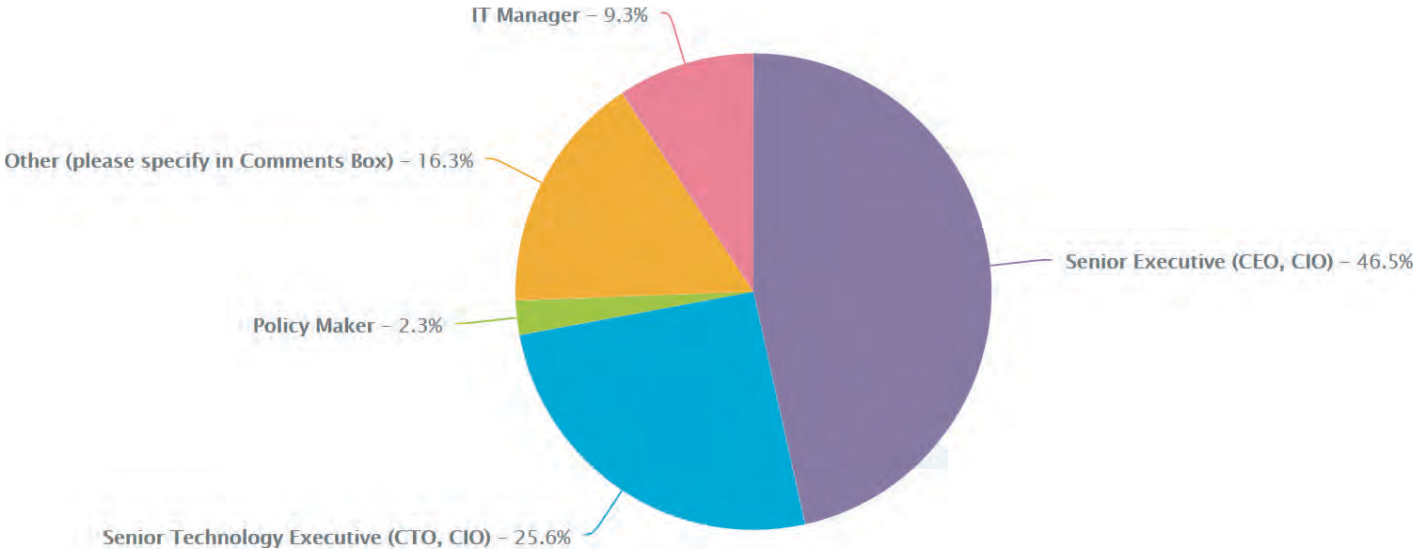
Cybersecurity must be considered wherever digital data and systems are used, but it should be managed centrally with focused responsibility and authority. Where cybersecurity management resides within an airport's organizational structure varies based on the existing organizational structure, the current placement of skilled staff members, management philosophy, and other factors. Airports indicated that the individual(s) responsible for cybersecurity within their organization report to a variety of managers, as shown in Figure 6. Those that responded "other" indicated the positions of administrative services director, chief financial officer or budget director, and vice president of commercial management.

The responses summarized in Figure 6 indicate the variety of places that cybersecurity can be placed within an organization. It also indicates the split of cybersecurity falling within the IT function versus reporting directly to senior management. This option was highlighted by many respondents during interviews and follow-up conversations. Because cybersecurity is largely, although not entirely, focused on digital data and systems, it requires skills sets that are typically found in IT functions within airports. That said, several respondents felt that cybersecurity is about risk management and should therefore report to the executive(s) responsible for organizational risk.

The titles that organizations give to the individuals they entrust with managing cybersecurity risk also indicate the variety of options that exist but are generally split between IT, senior management, and security. Titles of the individuals responsible for cybersecurity include chief information officer, chief security officer, IT manager (responsible for cybersecurity), and others. Increasingly organizations are establishing specific cybersecurity positions with the title of chief information security officer (Strahler 2014).

Funding

Funding is an important resource that is required to implement and sustain an effective cybersecurity program. It is required to compensate staff members and to procure products and



Source: 40 of 51 organizations that responded to the survey or interviews conducted for this project.

Figure 6. To whom does cybersecurity report?

services from the necessary cybersecurity service providers. As with human resources, the level that is required must be estimated and sources must be found to fill any gaps to what is available. The costs and benefits of cybersecurity must also be considered to determine the level and sources of funding required.

Funding Levels

Unfortunately, cybersecurity budgets have traditionally been a relatively low portion of an organization's overall IT budget (based on survey results from this project as well as NCHRP 20-59(48), "Effective Practices for the Protection of Transportation Infrastructure from Cyber Incidents"). Airports also report that the IT budget is typically less than 10% of their overall operating budget [based on 13 of 18 (72%) respondents who answered the question]. Even with the largest airports' operating budgets in the hundreds of millions (City of Chicago 2014; Greater Orlando Aviation Authority 2014; Dallas/Ft. Worth International Airport 2014; Minneapolis–St. Paul Metropolitan Airports Commission 2014), cybersecurity expenditures can quickly be diminished to relatively small levels.

Airport cybersecurity budgets are however on the rise [7 of 24 (29%) respondents indicated their budgets would rise 5% or more and 12 of 24 (50%) respondents indicated their budgets would rise 1–5%]. These increases are driven largely by the desire to prevent service interruptions, property damage, data loss, or degraded reputation.

Estimating the specific amount of funding required is difficult because each airport's budget priorities and propensity to spend on cybersecurity protection will be different. Considering the range of staff FTEs that may be required, an annual cost of $50–500 million may be required to support staff time spent on cybersecurity activities. A rudimentary top-down estimate using the percentages cited previously from the project survey responses suggests airports spend 0.9% of their operating budget on cybersecurity. Based on median airport operating expenses, this may equate to as much as 10 to 12 cents per enplaned passenger. Caution: These rules of thumb are not based on a comprehensive statistical or cost analysis.

Funding Sources

Regardless of the level required, funding to support increased cybersecurity activities must come from somewhere. Following are the possible sources of funding that should be considered to support an airport's cybersecurity program:

- **Operating expenses** budget is likely the most common source of the funds airports use to support cybersecurity activities. Cybersecurity often falls under the IT budget of an airport and this budget is typically considered an operating cost.
- **Capital investments** are often used to fund large infrastructure or facility improvements. The cost of implementing countermeasures to protect the data and systems that are implemented as a part of these programs should arguably be incorporated into the cost of these programs.
- **Grants** from the DHS and other federal agencies to support cybersecurity activities are on the rise. Consistent with the Obama Administration's emphasis on cybersecurity, cybersecurity budgets of many federal agencies have been on the rise (Corrin 2013). Using federal budget appropriations, the DHS "will fund more cybersecurity research and help . . . local governments bolster their online defenses" (Sullivan 2013). Some of these funds may be indirectly available to support cybersecurity at airports. The Catalog of Federal Domestic Assistance (CFDA), which can be found at the CFDA website (www.cfda.gov/), lists available grants, several of which are intended to support cybersecurity research and training. State and local agencies are sometimes on the list of eligible applicants for these grants. One such cooperative program from DHS

provides funding that supports the MS-ISAC. Airports can become members in the MS-ISAC and can receive some cybersecurity services free of charge as a result. MS-ISAC also offers extended services for an additional fee.

Regardless of the amount of funding required or the sources used to provide that funding, it is incumbent on each airport's management to determine the proper level of cybersecurity spending based on the funds available, alternative uses of those funds, and their desire to protect their airport data and systems from cyberattack. This decision should be evaluated on an annual basis as budgets are determined with the assistance of IT and facility managers who are making investments in new or existing systems. It is also incumbent upon all involved in supporting an airport's cybersecurity program to make the most use of free or low-cost resources that can support their cybersecurity objectives.

Costs Versus Benefits of a Cybersecurity Program

A cybersecurity program does not need to be costly or complex or require resources beyond an airport's means. Any level of protection is better than no protection. An airport's senior management must decide the relative costs and benefits of a cybersecurity program and empower their staff to implement the level of countermeasures they feel are warranted. IT staff and consultants should work with their senior managers to provide them with the information they need to make an informed decision.

Because many countermeasures are free, low cost, or perhaps already in place, an airport can establish a basic cybersecurity program without a large initial investment. This document is intended to provide the guidance that airport managers need to be proactive in a way that follows best industry practices but provides an acceptable cost–benefit return based on the airport's other needs and available resources.

Many feel that senior managers should not expect a cybersecurity program to provide a positive return on investment. Cybersecurity is an increasing cost of doing business and of utilizing modern technology. It does not offer revenue, improve efficiencies, or allow staff to accomplish tasks they otherwise could not do. If return on investment must be measured to support corporate decision making, then benefits that may be measured include the avoidance of costs associated with a successful attack, and the associated operational downtime, fines, and recovery costs that would ensue. Such information is difficult to quantify and must be weighted by the likelihood of it occurring, which is even more challenging to measure. For these reasons, quantified cost–benefit analyses or return-on-investment calculations should be cautiously interpreted. Airports that require such analyses in order to make investment decisions should consider at a conceptual level the cost–benefit ratio of performing such an analysis. In this regard, cybersecurity is similar to physical security. It is a necessity, in some cases a legal requirement, and ultimately a prerequisite to operating an airport.

External Support

There are numerous external resources that can support an airport's cybersecurity program. There are a growing number and variety of vendors, consultants, and service providers that offer products and services. Many of these providers can augment or fulfill several of the roles required by an effective cybersecurity program. In addition to these paid service providers, there are a number of agencies that can provide direct or indirect assistance for free. Some of these can help an airport establish a cybersecurity program; some can provide ongoing assistance to sustain a cost-effective cybersecurity program; and others can help if a successful attack occurs.

Following is a list of such external agencies, listed in descending order of the number of survey respondents that mentioned beneficial relationships with such agencies:

- The **Federal Bureau of Investigation** has field agents assigned to airports. Cybersecurity is a large and growing part of the FBI's mission, and these field agents can provide airports with information on new threats as well as assist if a successful attack does occur. It is prudent to identify the airport's FBI field agent(s) and inform them about the airport's makeup, objectives, and actions related to cybersecurity. This can best be accomplished through continued contact between the airport and the local FBI office.
- The **Transportation Security Administration** has passenger screening and other physical security responsibilities at most airports. TSA is often the most visible part of the DHS at an airport. Since many cyberattacks are carried out by attackers on the airport premises, TSA can be a vital resource in identifying and reducing the likelihood of an attack.
- **Department of Homeland Security** has many offices that are focused on cybersecurity, although they are not necessarily located at the airport. DHS can provide airports with information about threats and may direct the airport to valuable resources in the event of a successful attack.
- **Local law enforcement** should be aware of an airport's cybersecurity activities and may be able to provide assistance in the case of a successful attack. A growing number of law enforcement agencies are developing cybersecurity units with personnel that are specifically trained to help organizations and individuals in their jurisdictions. Regardless of the assistance they can offer, cyberattacks are a crime and should be reported to law enforcement officials.
- The **Federal Aviation Administration**—whether on-site, at a regional office, or at headquarters—may be able to provide assistance in response and recovery depending on the nature of an attack.
- The **Central Intelligence Agency** (CIA), like the FBI, is increasingly focused on cybercrime and may provide information on new threats that airports may face.

It is prudent to not wait for an attack to occur to reach out to these agencies. Most airports [20 of 21 (95%) who responded to the question] have already established relationships with such agencies. By establishing relationships and allowing them to become familiar with an airport's cybersecurity objectives, staff, and activities, external agencies will be better able to provide effective assistance should an attack occur. The best way to achieve this is to have periodic meetings to which these individuals are invited. The contacts and relationships that evolve from such interaction not only will improve the cost-effectiveness of a cybersecurity program as it is getting started or operating normally but also can save vital time in the response and recovery to a successful attack.

Cybersecurity Training

Training is an important part of an airport's cybersecurity program. Many of the most common threats can be averted by providing training that increases awareness and encourages employees and consultants to constantly be vigilant. Training is also less expensive than many other countermeasures and far less expensive than recovering from a successful attack. Training is specifically called out in the NIST "Framework for Improving Critical Infrastructure Cybersecurity" (NIST 2014) and has been demonstrated to be a cost-effective approach to achieve an initial base level of cybersecurity protection. A user-focused cybersecurity education by a dedicated cybersecurity staff for all airport employees to make them aware of potential threats is critical to mitigating vulnerabilities, concludes a recent paper on Cyber Security for Airports (Gopalakrishnan et al. 2013).

The majority of organizations surveyed [20 of 27 (74%) that responded to the question] indicated they do have a cybersecurity training or awareness program for employees. Training

topped the list for cybersecurity best practices used or planned to be used in the next 12 months: cybersecurity training for staff (83% of respondents, 24/29). Because most of this training is being conducted by internal resources (90% of respondents, 26/29), the type, quality, and breadth of the training is not likely to be comparable from site to site. Despite the promise of planned training, based on the survey results, the following constraints limit the participation in, and the effectiveness of, a current or planned cybersecurity training program:

- **Insufficient information about available training** [3 of 7 (43%) that responded]: Lack of available training information should not be a barrier as casual search for cybersecurity training results in more available training than most organizations can synthesize. This may overwhelm a staffer that is already busy fighting day-to-day business issues at an airport operation. The multimedia segment of this report provides a first level of training and offers links to additional resources, some of them available at no or low cost.
- **Insufficient budget for staff overtime to take training or training contractors** [2 of 7 (29%) that responded]: A current approach to training is to provide training materials that are self-paced, online, and modular to allow a staff member to receive training in segments rather than providing an overtime budget for training. Just as mandatory communications meetings or organizational meetings occur within a department or group, training needs to be sanctioned by senior management as an integral component of an employee's work responsibilities. Also, for some positions, certifications (e.g., PCI DSS) are required as a minimum upon hiring and then annual re-certification is necessary. Budget for basic and advanced training does require the business to prioritize the risk/benefit and this is accomplished in the assessment phase of the NIST Framework.
- **Lack of management support** [2 of 7 (29%) that responded]: Increased visibility at the national level for protection of critical infrastructure (including airports) against cyber threats is precisely targeted at reaching the management and budgeting authorities. Studies do demonstrate that cyberattacks are now focusing on senior management because they might be more lax when it comes to IT mandates and requirements due to their busy schedules. For-profit companies are now seeing the pressure at the board level, which will ultimately motivate the management.
- **Confusing training requirements and lack of internal expertise to conduct training**: Almost two-thirds of survey respondents indicated their spending on training will increase or stay the same, so the awareness of the need appears to have made an impact on future investment. However airport personnel responded that the variety of training programs and sometimes conflicting standards present a barrier to decide what type of training should be implemented with their limited budget.

Types of training range from cybersecurity awareness designed for the entire organization to more specialized training for staff responsible for networks, development of internal applications, or financial and personnel information. A best practice is to provide awareness training to every new hire as well as an annual refresher course covering the changing threat landscape and recent attempts or breaches at other airports or in other transportation-related industries. Because of its foundational value, awareness training is the focus of the next section. Specific training for the hardware and software configuration of the individual airport should be part of the professional development and protection phase of the overall cybersecurity plan.

"People cannot value security without first understanding how much is at risk."
–White House (2009)

Awareness Training

At the national level, it has become clear that awareness of our cybersecurity threats and countermeasures is essential to creating an overall level of protection. Accordingly, NIST's Framework includes Awareness and Training as an important countermeasure. The Framework recommends that "the organization's personnel and partners are provided cybersecurity

awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements."

While awareness is important, airports that responded to this project's survey indicated that for the most part senior management is aware of cybersecurity but does not consider it a primary concern [4 of 9 (44%) that responded to this question] or that senior management is made aware when an issue occurs [3 of 9 (44%) that responded to this question]. For many, cybersecurity is not a priority until an attack. As illustrated earlier (see Chapter 3), cyberattacks on airports do occur and some have been successful.

Increasing cybersecurity awareness among senior management, airport staff, and tenants and consultants is an important foundation for other elements of a best practices plan. Fortunately, it is a relatively easy one to implement using this guidebook, the associated multimedia material, and the additional sources cited. Following are some of the steps that airport managers and staff who are responsible for cybersecurity can take to increase awareness:

- Require awareness training for all new hires
- Provide mandatory annual updates for all employees
- Initiate a method for assessment preferably pre- and post-awareness training
- Offer online availability of awareness information for referral
- Disseminate alert of any current, active, or suspected threats to all users
- Implement a reporting program for employees to notify the appropriate security department of phishing, spear phishing, suspected malware, anomalous behavior, etc.
- Provide a clear method for reinforcing behavior change by creating simulated attacks (for example, phishing emails) with immediate awareness training/feedback
- Create consistency through assessment of the progress of the organization toward awareness goals and publish the progress results to users

The multimedia material can be used to help increase the awareness of cybersecurity best practices within airport organizations.

Specialized Training

Personnel tasked with the management or control of specific systems (e.g., network infrastructure, financial data, PII, ICS) require specialized training unique to the configuration of the individual airport. Regulations govern only a small fraction of these. Breaches of PII are covered by laws in 47 states although no comprehensive federal legislation is in place. Legislation is being proposed that would extend regulations that currently only apply to government agencies or contractors to the government.

As an example of a practice that may apply in the future to airports receiving federal funding, the U.S. Department of Transportation and FAA are required annually to audit the state of the information security program as required by the Federal Information Security Management Act of 2002. The most recent report and audit indicated improvement in 2013; however, significant security issues and vulnerabilities were uncovered according to the final report of the FY 2013 audit. Training was among those mentioned.

The audit report specific to training states, "The Department successfully provided security awareness training to over 90% of its employees but had not made sufficient progress in other critical areas. In particular, programs are still not adequate to ensure that (1) all contractors

receive required security training and (2) personnel with significant security responsibilities receive sufficient specialized training" (FISMA 2013).

Airports, particularly small and midsized, may be vulnerable to consultants working on systems with insufficient specialized security training. Facilities project managers may not recognize the need for the involvement of IT and security personnel.

Training Resources

- **National Cyber Awareness System** (http://www.us-cert.gov/ncas/) offers an array of information for employees with varied technical expertise—all but the most technical and trained cybersecurity personnel. This material can supplement an awareness program and provide updates on the most current threats. Those with more technical interest (specifically IT staff responsible for configuring or monitoring network systems) can read or subscribe to Alerts, Current Activity, or Bulletins. These products can also be summarized and disseminated as part of the communication to less technically astute users to maintain a current secure posture. End users with less technical expertise who are looking for more general-interest pieces can read the Tips; alternatively, these Tips can be incorporated as appropriate into the ongoing airport awareness program. As a proactive part of an airport best practice awareness program, a staff member can be tasked with subscribing to, receiving, and disseminating the daily and weekly information as appropriate to the different members of the community, and maintaining a resource on the specialized cyber training intranet.
- **National Cybersecurity Workforce Framework** (http://csrc.nist.gov/nice/framework/) provides tools to identify the tasks and KSAs required of a qualified cybersecurity workforce and provides a current listing of training options that are available (NICE 2014).
- **Several universities** including Texas A&M Engineering Extension Service (https://teexweb.tamu.edu/) offer free or inexpensive cybersecurity training.
- **PCI-Essentials** (https://www.securityinnovation.com/training/cardholder-data-security/pci-essentials-awareness-training.html) is a modestly priced online course offered by the PCI's Security Standards Council. This course helps organizations attain a level of compliance with PCI DSS that credit card companies require.

Sustaining a Cybersecurity Program

Like all assets (tangible or not) a cybersecurity program must be maintained to protect the investment that has been made and, ultimately, to be effective in protecting the airport's data and systems. Ongoing training, monitoring, funding, and management support are required to sustain an active and robust program. This is particularly challenging when the threats, as well as the measures to counter those threats, are evolving so rapidly. The following ongoing activities are recommended to sustain an effective airport cybersecurity program:

- **Inventory updates** are required to reflect the current configuration of an airport's systems, information resources, and network infrastructure. This inventory should not only identify the data, systems, and devices but also track information that is critical to protecting these assets such as users, vendor, criticality of use, and other factors. Keeping this inventory up to date on a continuous basis not only ensures the details will be available when needed, but also avoids the repeated expenses of consultants being hired to perform comprehensive updates as part of an IT master plan.
- **Threat intelligence** must be kept up to date so that the likelihood of a successful attack against the information, systems, and devices inventoried is as current as possible. ISACs, relationships

with other agencies, dialogue with peer airports, and support from service providers are all ways to maintain a high level of threat intelligence.

- **Program budgets** should be periodically updated to ensure that staff and funding resources are available to implement the countermeasures required to protect the airport against current threats. Such budget decisions require that vulnerability assessments be updated to reflect the current landscape of threats and available countermeasures. Budget funding for cybersecurity may also change as awareness grows and attacks are experienced.
- **Software upgrades and patches**, particularly those that address a new or newly discovered vulnerability, should be applied as they are made available by vendors. Information on which versions of software and which patches have been applied should be recorded in the airport's systems inventory.
- **Continuous monitoring** of network activity, application, system, social media, and email logs is an ongoing necessity of a cybersecurity program. Airports that cannot or choose not to retain qualified staff to handle this activity can rely on service providers, as well as increasingly sophisticated software and hardware, which can alleviate the burden, albeit at a cost.
- **Vendor selection criteria** should ensure that airport cybersecurity requirements are met as new information services and systems are procured. This will require constant interaction with airport managers looking to procure new information services and products, as well as procurement managers who are responsible for including technical specifications as well as airport cybersecurity policies and procedures into solicitation and contract documents. Periodic confirmation that vendors on multi-year contracts retain the necessary skills, equipment, and procedures should be considered.
- **Training** needs to be an ongoing process not only to refresh staff, consultant, and tenant understanding of their roles and responsibilities but also to keep them up to date on the latest threat information. Periodic training is also a requirement of compliance with PCI DSS and should be determined if required for other regulatory or legal requirements.
- **Risks** that can limit the success of a cybersecurity program should be periodically considered. New risks should be identified and the effectiveness of mitigation strategies will need to be evaluated.

These activities should be carried out by the individuals who fulfill the variety of roles related to cybersecurity at an airport. These individuals should ensure that the necessary cybersecurity activities are executed in an efficient and effective manner.

Risk of Implementing a Cybersecurity Program

Few activities offer positive outcomes without some form of risk that must be mitigated to ensure optimal results. Cybersecurity programs are no exception. They introduce risks that need to be identified along with their potential impact, likelihood of occurrence, and steps that can be taken to mitigate them. Following is a list of potential program risks that a CISO or the individual(s) entrusted with leading an airport's cybersecurity program must manage for that program to be effective:

- **A false sense of security** may arise among airport managers and staff once investments in cybersecurity have been made. The result can be reduced vigilance in carrying out countermeasures, observing anomalous activity, and reporting suspected attacks. Periodic training and reminders that highlight new threats and the importance of continued support can reduce the likelihood of this risk to a cybersecurity program's effectiveness.
- **Increased visibility** can result from greater organizational emphasis on cybersecurity. This may increase the awareness and interest of nefarious actors, from outside or inside an organization. To minimize this risk, information on cybersecurity vulnerabilities and countermeasures

should be treated as SSI and be made available to only those who need to know and who have agreed to handle this information in a specific manner.

- **Overreaction to threat** may result from increased awareness of cybersecurity threats; for example, threats highlighted in the media may create a sense of panic or at least overreaction that may overly influence decisions to invest in data and systems. Ultimately, the objective of technology is to serve a variety of needs. The use of technology should be protected against cyber threats but not in an overly limiting manner. To address this, vulnerabilities should be assessed and prioritized on an ongoing basis by informed experts from within the airport or external service providers.
- **High turnover rates** may occur after airport cybersecurity staff members are trained and gain valuable experience at the airport. The rapidly growing demand for cybersecurity professionals and the current shortage of qualified human resources may lead to a high turnover rate among airport cybersecurity staff. Cybersecurity programs need to mitigate this by managing workloads and creatively attracting and retaining top talent. A balanced approach includes flexible work hours, competitive compensation packages, and constantly challenging qualified people with a variety of tasks.
- **Poor return on investments in vendor products** may result if the products and services being offered are not thoroughly evaluated. Whether building a new program or maintaining an existing program, airport managers are being presented with a growing range of emerging cybersecurity products and services. Aggressive sales and marketing campaigns fueled by growing market demand, often make it appear that these new products and services are essential. To mitigate this risk, those involved in procuring cybersecurity products and services should carefully evaluate the choices, seek testimonials and reviews from peer organizations, and carefully consider the costs and benefits of each solution.
- **A reluctance to spend money on cybersecurity** may arise, especially during tight budgetary times, after the initial investment in a cybersecurity program is made. Because the impact and effectiveness of a cybersecurity program is difficult and time consuming to quantify, cybersecurity programs may become seen as an unnecessary expense. The irony of avoiding successful attacks is that senior management and others may perceive the threat level to be lower than it really is because they are experiencing the benefit of the past investments that have been made and should therefore be sustained. Mitigating this risk requires information and metrics of the threat levels that exist and the criticality of the data and systems that could be affected at the airport if a successful attack occurs.
- **Information overload** is increasingly likely as airport managers subscribe to and pay more attention to the growing information that is available on cyber threats. In many situations the information that is available becomes so pervasive that managers do not have time to review the portions that are relevant to their airport. To overcome this, specific individuals should be tasked with reviewing and interpreting the information that is received. They can then forward or highlight the relevant pieces to the appropriate parties. Care should also be taken to subscribe only to the resources that are most likely to provide relevant information.

The individuals entrusted with cybersecurity at an airport must identify these and other risks the programs they manage may face. They should develop, implement, and periodically reevaluate the effectiveness of the mitigation strategies they develop to reduce the likelihood and the impact of these risks.

CHAPTER 6

Detecting, Responding to, and Recovering from Attacks

This chapter describes techniques that airports can follow to detect, respond, and recover from cybersecurity attacks. More than a few experts interviewed for this study noted that "it is no longer a question of if your organization will be attacked, it is a question of when." This is where all of the practices described previously in this document yield value. The objective is to detect an attack that has occurred as soon as possible, respond quickly and efficiently, recover to a normal state of operations with as little disruption as possible, and learn lessons to prevent similar attacks in the future.

It is no longer a question of if your organization will be attacked, it is a question of when.

Attacks are threats that have been realized, whether they have been successfully averted by countermeasures or not. Those that have been averted should be noted so that trends can be identified. Successful attacks that have not been averted require immediate response. After the organization has recovered, additional countermeasures should be put in place to ensure that the uncovered vulnerability is addressed. The following sections describe detection, response, and recovery practices that airports can follow to achieve these objectives.

Detecting Attacks

Cybersecurity attacks, such as advanced persistent threats, can occur undetected and reside within an airport's network for long periods of time. During this time, information that the airport considers sensitive or confidential may be leaked, or malware may be installed for activation at a later date. "Identifying whether an attack has occurred can be incredibly challenging," remarks Rob Lee, the Digital Forensics and Instant Response Lead at SANS Institute (Karol 2013). He further notes that statistics from Madiant indicate that it takes companies an average of 416 days to detect a cybersecurity breach (Karol 2013). Regardless of whether such lingering attacks occur or not, it is prudent for airports to make every attempt to detect attacks that occur as quickly as possible. Following are some practices that can help achieve that goal:

- **Anomalous activity** should be reported and analyzed to determine if it is benign or malicious. Anomalous activity is system, device, or network behavior that differs from the norm. Activity such as slow response and refresh rates, inappropriate information and controls (e.g., links, pop-ups, entry boxes) on a website, and redirection to suspicious domain names may be observed by users. It can also involve network activity that trained cybersecurity professionals may notice, such as connections to IP addresses not required by an application, scanning of ports and services on a network, user logins to unusual systems or at unusual times, simultaneous login attempts using one set of credentials, and abnormally large data downloads (DarkTrace 2014). In order to determine what activity is anomalous, it is important to first understand what activity is "normal" (Stotts and Lippenholz 2014). Martin Roesch, founder of SourceFire, a cybersecurity services provider, explains "once you're aware of how your network works, the applications people use, and the amount of bandwidth they chew up, you'll

be able to spot anomalies that will help you identify an attack" (Karol 2013). This baseline is defined by details such as what applications and systems communicate over what ports, which users have access to specific applications, and typical ranges of network speed and data transfer volumes. This information should be collected and documented by IT professionals as a part of the inventory described earlier. Anomalous activity may be detected by continuous monitoring (described in the next list item) or by users who should be encouraged as a part of cybersecurity training to report computer or network behavior that they feel is outside the norm.

- **Continuous monitoring** involves software and hardware installed on premises or at a cloud-based provider that monitors application, database, system, and network activity. Events, data requests, login attempts, port scans, and other activities are recorded in logs that can be analyzed by increasingly sophisticated software and trained professionals. Monitoring tools and services are rapidly being developed to confront growing frequency and sophistication of cyber threats. Some of the options can be very expensive, while others are less expensive or in some cases free. It is outside the purview of this document to recommend vendor solutions. Furthermore, such recommendations would rapidly become out of date. It is therefore recommended that airport cybersecurity professionals become acquainted and remain up to date with industry product and service offerings. They should also talk with peers at other airports to gain referrals and testimonials regarding offerings that have or have not worked.
- **Event triggers** can be set on software and systems to alert IT staff or third parties of activity that strays outside of acceptable norms. Care should be taken to ensure that an abnormally high rate of false returns does not overload the individuals tasked with responding and cause them to become complacent. At the same time, the triggers should not be set so tight that activity that should be reviewed is not identified. Penetration testing is used to determine if triggers will detect the events desired.
- **Antivirus and malware detection software** should be installed on end-point systems such as desktops, laptops, and mobile devices. While these tools do not always catch known threats targeting these devices (Stotts and Lippenholz 2014), those that are detected should be recorded to identify trends or related activities that may be more successful.
- **Inappropriate behavior** of humans is an anomalous activity that all staff, consultants, and tenants should be trained to observe and required to report. Individuals trying to gain access to areas where secure systems or network infrastructure are present should be reported to security personnel. Similarly, individuals appearing to observe others to gain information such as passwords or to steal sensitive documents should also be reported.

Cybersecurity detection should not be limited to detecting attacks, whether successful or not. Countermeasures that are not implemented or carried out as required should also be observed, reported, and remedied. In some cases, airport staff members, consultants, and tenants will be able to identify countermeasures that are not implemented properly. In other cases, a trained staff member is required. Common examples of countermeasures not being carried out include the following:

- **Not following policies or procedures** that are designed to implement countermeasures such as the handling of SSI, not writing down and displaying passwords, and browsing non-work-related sites. Such infractions should be reported and recorded not only as a means of addressing individual infractions but perhaps more importantly to improve awareness and training so that they do not continue to occur.
- **Not attending training** will likely cause staff members to forget some of the policies and procedures they are required to carry out and not be familiar with the latest threats, and the airport may fall out of compliance with contracts and regulation. To avoid this, employees should be required to periodically attend training and records of their attendance should be kept.
- **Contracts and agreements** should be reviewed to ensure that airport policies, procedures, and specifications with regard to cybersecurity are properly incorporated. Not only procurement

managers but also the IT and facility project managers, who may be more familiar with the technical requirements, should conduct these reviews.

The detection of attacks and inappropriately applied countermeasures is a large but critical task. Individuals who fulfill the roles defined earlier in this document should participate to the extent that they are technically able. This responsibility should be conveyed and made clear to them as a part of required cybersecurity training. Even with such a concerted effort, airports may need to seek help from outside service providers. "It's difficult for [most government and commercial entities] to build and maintain the infrastructure and capabilities needed to effectively monitor and analyze data on hundreds of thousands of systems on a daily basis," note Richard Stotts and Scot Lippenholz of Booz Allen Hamilton. This is due to staff availability and the need to keep up to date with cybersecurity threats and available countermeasures. Fortunately, organizations focused on this mission such as the DHS, FBI, CIA, local law enforcement agencies, ISACs, and a wide variety of vendors are able to assist.

Responding to an Attack

A cybersecurity program should have a process in place to quickly and effectively respond to cybersecurity attacks while minimizing the duration of their impact. The first objective in a response is to identify the data and systems that are affected as well as the vector used to circumvent countermeasures. The second objective is to communicate the information that is known to relevant stakeholders and to collaboratively carry out an effective response. This response should contain the attack to the data and systems already affected to the extent possible and then close the vector used by the actor to limit further infiltration. To achieve these objectives, the following steps should be carried out:

- **Collect data** from logs and users. Scans of potentially affected systems should be conducted to provide additional information. External contact with agencies and peer airports may also provide information on known threats or similar attacks experienced by others. Depending on the severity and complexity of the attack, a digital forensics examination by a qualified third party and interaction with law enforcement officials may be warranted.
- **Analyze** the information collected from the previous step to understand the impact of the attack as well as the vector that successfully avoided countermeasures. The impact analysis should span affected systems as well as other connected systems and network devices. Using this information, the investigator should attempt to understand the motive of the attack, such as stealing confidential information, disrupting operations, or damaging the airport's reputation. Consideration should also be given to the tools, techniques, and methods used to deliver its malicious payload to the compromised system or infrastructure component.
- **Containment** should be applied to temporarily or permanently close the attack vector used, isolate any malware or corrupt data that could cause further harm, and restrict users from relying on affected systems until a recovery to normal operations is complete.
- **Communicate** that the attack has occurred and any relevant details to senior management, affected parties, those who can assist, and law enforcement officials. Some of the information about the attack and even the fact that an attack has occurred may be considered SSI or confidential. Accordingly, information should be shared with the appropriate stakeholders according to a pre-defined communication plan. Contacts at relevant agencies should already have been established so that those who can help are already familiar with the airport's data and systems to the extent they need to be. Third party service providers should already have been identified, and if possible under an on-call contract, so that they can be quickly brought in to assist. Senior management and legal staff should also review and approve any potentially sensitive information before it is released. Some information may even result in legal action against the airport if victims or even attacker(s) are inappropriately identified.

All response activities should adhere to the airport's policy and procedures. Since time is of the essence during a response, individuals who fulfill the roles required during a response should already be aware of and trained on these policies and procedures. External resources should be considered and perhaps already under contract to assist in a response. Often such external resources have specialized training, experiences, and resources needed to effectively respond and recover.

Responding to a cyberattack demands immediate time and attention, especially from those whose task it is to protect the airport. The challenge is for those resources to not divert so much of their attention to the attack that it causes them to let their guard down, which could increase the likelihood of another, possibly more harmful attack. This need to maintain countermeasures during the response to a successful attack should be taken into consideration when deciding to tap external service providers in response and recovery activities (Stotts and Lippenholz 2014).

Recovery to Normal Operations

After the immediate response has contained the attack and appropriate stakeholders have been alerted, steps should be taken to bring the organization back to a normal state of operation as quickly and efficiently as possible. Disrupted operations and associated reputational losses are among the negative effects that can be minimized by a quick recovery.

As with detecting anomalous activity, it is important to have a clear idea of what normal operations means before attempting to achieve that goal. What systems should be operational, what data is needed, and which users need access to which systems are questions that should be answered and documented long before an attack occurs. These normal data, systems, and capabilities should also be prioritized so that the most critical and widely used can be addressed first in the recovery process. The recovery of these and eventually of all affected data and systems can then proceed with the following steps:

- **Remove infectious software and corrupt data** permanently from systems that have been affected. Infectious software can include malware, worms, and other forms of code that infiltrate a network and enable data to be stolen, corrupt data, or disrupt system operations. Such code can often linger for long periods of time before it is detected. Attempts to contain the problem during the initial response may be temporary or may restrict valid capabilities that need to be reinstated to attain normal operations. Eventually, the infectious code should be removed permanently. In some cases, antivirus, malware, and spyware detection software can accomplish this, but with more sophisticated attacks, this may be difficult if not impossible. It is often more efficient to isolate and then rebuild an infected system. This process is facilitated by using virtual machines that can be imaged and then quickly reinstated using a backed-up image.
- **Recover data, software, or systems** from archived backups. Information in the form of digital files and database records should be frequently backed up, so that if they need to be recovered little data is lost. This frequency depends on how often the data is updated and the cost of recovering updates that may be lost between backups. Software can be reinstalled, but any local configurations should be saved and backed up where possible. Entire systems can be rebuilt, although this can be a time-consuming process. One of the advantages of using virtual machines is that an entire image of a machine encompassing the operating system, software installed, and data can be quickly restored with little or no reconfiguration.
- **Reauthorize access to data and systems** that may have been isolated during the containment step of a response. This may involve reinstating user access rights, reopening network communication ports and protocols, and bringing systems back online.
- **Reset credentials** that may have been compromised as the result of an attack. Stealing user access credentials as a means of gaining access to sensitive data, other systems, or money is a

common goal of an attack. If such credentials are or are suspected of being lost, they should be reset so that users have to establish new passwords or are issued new user identifiers.
- **Inform users** that their data and systems have been recovered and that they can resume operations as normal.

Other steps may be required based on the nature of the attack and the degree of impact. The documentation that describes the normal state of operations can be used as a guide to identify additional recovery activities that may be required.

The just described recovery activities should be reflected in a response and recovery plan. Continuity of operations (COOP) plans are one such type of plan, which was initiated by the federal government during the Cold War and formalized by National Security Presidential Directive 51 and Homeland Security Presidential Directive 20. These plans ensure that "Primary Mission-Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies." These directives require federal agencies to take such an approach, but transportation organizations have found them relevant to the response and recovery to cyberattack.

Less than a quarter of the organizations surveyed by this project and a similar one [NCHRP Project 20-59(48)] conducted for transit and highway transportation organizations [14 of 63 (22%) who responded to the question] indicated that they have a COOP plan for their transportation operations systems. Slightly more [17 of 63 (27%) who responded to the question] indicated that they have a COOP plan for their enterprise data systems. A higher percentage of respondents [23 of 63 (37%)] have a COOP for both operations and data systems. Regardless of whether a formal COOP plan is established, a documented plan to respond and recover from cybersecurity attacks is recommended for airports.

Lessons Learned

An organization that has successfully been attacked should not return to normal operations as defined by the state of operations prior to the attack. New countermeasures, some of which may alter activities previously defined as "normal," may need to be implemented.

The second part of the old adage "fool me twice, shame on me" should be ample motivation to implement new countermeasures to prevent the same attack from affecting an airport more than once. In reality, attackers are constantly learning lessons as well and the vector, targets, and vehicles used to carry out a successful cyberattack may not be repeated in exactly the same manner. It is therefore important to learn lessons from attacks on one's own organization as well as peers and competitors, whether those attacks were successful or not. Information sharing has proven to be one of the most effective countermeasures in the financial services industry, where competitors share lessons learned to benefit the entire industry.

These lessons learned should be applied to change policies, procedures, and implement new or improved countermeasures. The efficiency and effectiveness of the response and recovery from an attack should also be reviewed to make improvements for the future. Metrics that attempt to quantify the cost of the attack in terms of operational downtime, loss of data and reputation, response, and recovery should also be recorded to reassess the return on investment that additional measures may provide. Senior management should also reassess their willingness to tolerate cyberattacks and make future investment decisions accordingly.

CHAPTER 7

Conclusions and Suggested Research

The following primary conclusions of this research are focused on steps airports can take to protect themselves against cyber threats. Additional research to help airports sustain this level of protection into the future is also recommended.

Conclusions

The growing threat of cyberattack on airport computers, networks, control systems, and critical infrastructure is a clear trend that is well publicized in the media, trade forums, and legislation. This trend is also substantiated in the research that has been conducted for this project. Cyberattacks are increasing in number and sophistication. The result has been a loss of confidential and sensitive information, costly disruption to operations, adverse impacts to reputation, and in some cases financial loss and equipment failure.

Fortunately, the number and sophistication of countermeasures to combat the increased threat is also growing. Federal, state, and local government agencies are passing legislation and offering resources to help. Non-governmental and non-profit organizations are establishing forums for information exchange. For-profit companies and individual consultants are also improving the services, software, and hardware they offer to combat the threats that exist.

No airport is immune to attack, and many can be better prepared. Implementing cybersecurity countermeasures is not an option; it is a requirement of safe and efficient operation. Following are some of the primary countermeasures that all airport managers and staff should consider:

- 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 ISACs, and engaging (if the means exist) cybersecurity professionals.
- Establish and enforce policies for acceptable use, SSI, information privacy, software and data assurance, training, and communications.
- Periodically train managers, staff, consultants, and tenants on their roles to protect data and system credentials, be wary of social engineering tactics, adequately protect the devices they control, and report suspicious activity and policy infractions.
- Maintain an inventory of data, systems, network devices, and users that may be affected by a cyberattack.
- Identify vulnerabilities where these assets are not adequately protected and prioritize them based on the impact a successful attack may have.
- Implement countermeasures to achieve the level of protection that is desired and affordable.
- Assign CISO responsibilities to a qualified staff member, new hire, or consultant.
- Monitor computer and human behavior through manual and automated means.
- Communicate anomalous activity and successful attacks to the CISO, IT staff, senior management, affected stakeholders, other agencies, and law enforcement personnel.

- Be prepared to isolate affected systems, remove them, recover from attacks, and learn from them.
- Recognize that even if all of the foregoing measures are implemented, the airport will still not be perfectly protected. Remain vigilant and continuously improve the level of protection to the extent possible given the resources that are available.

To implement these and other countermeasures in an effective manner, many airports are establishing cybersecurity programs led by a CISO and supported by senior management. Such an approach formalizes the process and establishes a centralized resource.

Cybersecurity is not out of reach for any airport. Whether the smallest general aviation or the largest hub airport, the challenge is to achieve a level of protection that provides those responsible for safety and operational efficiency with a desired level of comfort within the limits of available staff and financial resources. While there are some laws and regulations that must be met, there are a wide variety of options based on the risk propensity, exposure, and resources available. Senior managers cannot, however, decide on the desired level of protection without input from technical and operational staff who understand the vulnerabilities and potential impacts of an attack. CISOs cannot implement the desired protection without this guidance; allocated resources; and the support of staff, consultants, and tenants. Protecting an airport from the threat of cyberattack is a shared responsibility and not one handled exclusively in the IT equipment room.

Airports need not pursue cybersecurity protection alone. There are a growing number of agencies, organizations, companies, and forums that can help. Some are emerging to specifically help airports and other aviation organizations. Following are some of the resources airports should tap in pursuit of a cost-effective cybersecurity program:

- **FBI agents** are assigned to each airport and can be a conduit to the cybersecurity resources of their agency.
- **DHS** provides funding that allows the MS-ISAC to provide member airports with training, material, and other resources as well as assistance should an attack occur. MS-ISAC also offers network monitoring and other specialized services for a fee.
- **Training resources** that are free or inexpensive but effective are increasingly available. Many of these are available online. Some that airports may find useful are listed in the cybersecurity training resources section of Chapter 5.
- **SANS Institute** (http://www.sans.org/reading-room/) offers an online reading room that is continuously updated with helpful documents.
- **InfraGard** (www.infragard.org) is a partnership between the FBI and the private sector that is dedicated to sharing information on hostile acts against the United States, including cybersecurity attacks.
- **CSET** is a CD-based software tool that helps organizations evaluate the cybersecurity posture of their systems and network. It was developed by DHS in conjunction with the ICS-CERT and NIST. It can be obtained free of charge from ICS-CERT (ics-cert.us-cert.gov/Downloading-and-Installing-CSET).

The guidance provided in this document, along with the multimedia materials offered and the growing number of industry resources available, should allow airports to determine, implement, and sustain a prudent level of cybersecurity protection.

Suggested Research

The research conducted during this project has identified best practices and steps that airports can take to protect themselves against cyberattack. The environment is however rapidly changing in terms of the threats that exist, data and systems that must be protected, and the

countermeasures available to help. This suggests that additional, and perhaps in some cases, ongoing research is required. Following are some suggestions identified during the course of this research:

- Threat analysis requires ongoing research into the actors, vectors, and types of threats that can affect airports. This analysis should include threat trend analysis, actor profiling and attribution, and system vulnerability testing. There are many agencies, organizations, and companies that are dedicated to this activity, but few if any are focused on airports. Support for an ongoing research initiative that pools threat information relevant to airports is therefore recommended. These need not, but perhaps would best, be established as a part of other broader research efforts.
- Technical standards and specifications for protecting ICS could be developed to help not only airports, but also installers and manufacturers of these systems, attain a common baseline of protection.
- Training for facility managers and ICS installers on how to protect their systems against cyber threat will help ensure those systems are properly protected. This training must include cybersecurity awareness and an overview of the airport's approach to protecting critical systems. In addition, the training should provide details on how to adhere to the specifications described previously.

These and perhaps other research efforts will help airport managers and staff remain vigilant despite the dynamic nature of cybersecurity.

Glossary, Abbreviations, Acronyms, and Symbols

Glossary

Actor—An individual or group that can manifest a threat.

Attribution—Information on an actor, primarily to specify their identity, location, motives, and level of sophistication.

Countermeasure—An action, device, procedure, or technique that reduces a threat, vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

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.

Defense in Depth—The implementation of multiple layers of countermeasures as a means of providing additional protection should one layer fail.

Industrial Control Systems—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).

Insider Threat (malicious)—A current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems (Carnegie Mellon University 2014).

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).

Vector—The channel or conduit by which an attack is carried out, including email, malware, physical access, and other means.

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).

Worm—A type of infectious software that replicates itself in order to spread to other computers. It is typically propagated by replicating itself using computer networks and exploiting vulnerable systems. Unlike viruses or other types of malware, worms do not need to attach themselves to an existing code base, and they may potentially damage both network devices and computer systems. The most important protection against worms is user awareness which is enhanced by antivirus software deployment. Removing a worm is a tedious process that starts with a comprehensive outbreak analysis that will lead to isolating infected systems and then applying the latest system recovery process.

Abbreviations and Acronyms

ACI-NA	Airports Council International–North America
ACRP	Airport Cooperative Research Program
AES	Advanced Encryption Standard
AFDX	Avionics Full Duplex Switched Ethernet
A-ISAC	Aviation Information Sharing and Analysis Center
AVI	Automatic Vehicle Identification
BCS	Building Control Systems
BIDS	Baggage Information Display Systems
BIT	Business Information Technology Committee
BYOD	Bring Your Own Device
CARMA	Cybersecurity Assessment and Risk Management Approach
CCTV	Closed Circuit Television
CDE	Cardholder Data Environment
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
COOP	Continuity of Operations
COTS	Commercial off the Shelf
CRUD	Create, Retrieve, Update, and Delete
CSET	Cyber Security Evaluation Tool
CUPPS	Common Use Passenger Processing Systems
CUSS	Common Use Self-Service
CUTE	Common Use Terminal Equipment
DCS	Distributed Control Systems
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
EFB	Electronic Flight Bag
ERAU	Embry-Riddle Aeronautical University
FBI	Federal Bureau of Investigation
FIDS	Flight Information Display Systems
FISMA	Federal Information Security Management Act
FTE	Full-Time Equivalent
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act
HUMS	Engine Health and Usage Monitoring Systems

ICS	Industrial Control Systems
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention Systems
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
KSAs	Knowledge, Skills, and Abilities
LAN	Local Area Network
MDM	Mobile Device Management
MS-ISAC	Multi-State Information Sharing and Analysis Center
NACS	Network Access Control System
NCIC	National Crime Information Center
NERC	North American Electric Reliability Corporation
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
PAC	Programmable Automation Controller
PARCS	Parking Access and Revenue Control Systems
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standards
PII	Personally Identifiable Information
PLC	Programmable Logic Controller
POS	Point of Sale
PSK	Pre-shared Key
SCADA	Supervisory Control and Data Acquisition
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMS	Short Message Service
SQL	Structured Query Language
SSI	Sensitive Security Information
SSL	Secure Sockets Layer
TRB	Transportation Research Board
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WIPS	Wireless Intrusion Prevention System
WPA-2	Wi-Fi Protected Access

Symbols

The following symbols have been used in this document:

- Threat
- Countermeasure
- Resource
- Target
- Multimedia

References

Airport Consultants Council 2012. *Airport Information Technology & Systems (IT&S) Best Practice Guidelines for the Airport Industry.* Jan.

AirTight Networks 2012. "Impact of Bring Your Own Device (BYOD)." www.airtightnetworks.com. Apr.

Asian Age 2014. "Airports Authority of India Conducts Security Audit After Hacking." *The Asian Age.* www.asianage.com/india/airports-authority-india-conducts-security-audit-after-hacking-640. 24 Sept.

Battey, J. 2014. "FAA Moving to Secure Microsoft Cloud." Computer Sciences Corporation. www.csc.com/public_sector/publications/91598/91642-faa_moving_to_secure_microsoft_cloud (As of Nov. 16, 2014).

Bodeau, D., Boyle S., Fabius-Greene J., and Graubar R. 2010. "Cyber Security Governance." MITRE Technical Report MTR100308. The MITRE Corporation. Sept.

Butler, B. 2014. "Even the Most Secure Cloud Storage May Not Be So Secure, Study Finds." *Network World.* Web. 21 Apr.

Byres, E. 2012. "SCADA Security Basics: SCADA vs. ICS Terminology." *Tofino Security.* www.tofinosecurity.com/blog/scada-security-basics-scada-vs-ics-terminology. 5 Sept.

Camhi, J. 2014. "State Governments & the Future of Cyber Security Regulation." *Information Week's Bank Systems & Technology.* 9 Jul.

Cappelli, D. 2012. "The CERT Top 10 List for Winning the Battle Against Insider Threats." Presented at the RSA Conference 2012, San Francisco, CA.

Cappelli, D., Moore, A., and Trzeciak, R. 2012. *The CERT Guide to Insider Threats.* Boston: Addison-Wesley Professional.

Carnegie Mellon University 2014a. "Insider Threat." Community Emergency Response Team (CERT), Software Engineering Institute. www.cert.org/insider-threat/ (As of Nov. 21, 2014).

Carnegie Mellon University 2014b. "Insider Threat Test Datasets" Software Engineering Institute. www.cert.org/insider-threat/tools/index.cfm (As of Nov. 18, 2014).

Center for Internet Security 2013. "2013 Annual Report." East Greenbush, New York.

Cheong, B. 2011. "Cyber Security at Airports." Presented at the Airports Council International–North America Conference. Oct.

Christey, S. 2011, "CWE/SANS Top 25 Most Dangerous Software Errors." The MITRE Corporation. cwe.mitre.org/top25/ (As of Oct 30, 2014).

CIRT.net 2014. Default Passwords. cirt.net/passwords (As of May 2014).

Citrix 2012. "Best Practices BYOD Simple and Secure." www.citrix.com/content/dam/citrix/en_us/documents/oth/byod-best-practices.pdf. Sept.

City of Chicago 2014. "Comprehensive Annual Financial Report for the Year Ended December 31, 2013." 30 June.

Committee on National Security Systems 2010. "National Information Assurance Glossary 2010, Instruction No. 4009." 26 April.

Corrin, A. 2013. "Budget Shows How Cyber Programs Are Spreading." *Federal Computer Week.* fcw.com/articles/2013/04/12/budget-cybersecurity.aspx. 13 Apr.

Dallas/Ft. Worth International Airport 2014. "Dallas/Ft. Worth International Airport FY 2015 Adopted Budget." Finance Department. Texas.

DarkTrace 2014. "What Darktrace Finds: Example Anomalies." www.darktrace.com/proven-track-record/example-anomalies/ (As of Oct. 22, 2014).

Depner, H. 2014. "Home Depot: Yet Another Retail Breach. PCI Compliance Just Doesn't Cut It." Blog post. *Kaseya.* http://blog.kaseya.com/blog/2014/09/03/home-depot-yet-another-retail-breach/. 3 Sept.

Dugan, D., Berg, M., Dillinger, J., and Stamp, J. 2005. "Penetration Testing of Industrial Control Systems." Sandia Report SAND2005-2846P. Sandia National Laboratories. 7 Mar.

Energy Sector Control Systems Working Group 2014. "Cybersecurity Procurement Language for Energy Delivery Systems." Apr.

Fischer, E. 2013. "Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions." Congressional Research Service. 20 Jun.

FISMA 2013. DOT Has Made Progress but Its Systems Remain Vulnerable to Significant Security Threats. Office of Inspector General Audit Report, November 22.

Francy, F. 2014. "The Aviation Information Sharing and Analysis Center." Presented at the ICAC Conference. 15 Sept.

Gartner, Inc. 2013. "Gartner Says Cloud Computing Will Become the Bulk of New IT Spend by 2016." Press Release. 24 Oct.

Gilliland, A. 2014. "Enterprise Security Products." Presented at RSA Conference 2014.

Glasser, J. and Lindauer B. 2013. "Bridging the Gap: A Pragmatic Approach to Generating Insider Threat Data." *Security and Privacy Workshops, 2013 IEEE,* pp. 98–104. Institute of Electrical and Electronics Engineers. doi:10.1109/SPW.2013.37.

Gopalakrishnan, K., Govindarasu, M., Jacobsonson, D., and Phares, B. 2013. "Cyber Security for Airports." *International Journal for Traffic and Transport Engineering,* 3(4): pp. 365–376.

Guttman, B. and Roback, E. A. 1995. *An Introduction to Computer Security: The NIST Handbook.* NIST Special Publication 800-12.

Honorof, M. 2013a. "Why the NSA's PRISM Program Shouldn't Surprise You." *TechNewsDaily.* www.technewsdaily.com/18291-prism-shouldnt-surprise-you.html. 7 Jun.

Honorof, M. 2013b. "How to Secure Your Cloud Storage." *Tom's Guide.* www.tomsguide.com/us/howto-secure-cloud-storage,review-1799.html. 29 Jul.

HSN Consultants, Inc. "The Nilson Report." Issue 1024, Aug.

IBM 2014. IBM Security Services 2014 Cyber Security Intelligence Index.

Information Security Standards 2014. Summary of ISO/IEC 27002:2013. IsecT Ltd. www.iso27001security.com/html/27002.html (As of Oct. 23, 2014).

Infosecurity Magazine 2008. "Cyber Security Lacking at Airports." www.infosecuritymagazine.com/news/cyber-security-lacking-at-airports/. 7 Mar.

Infrastructure Security and Energy Restoration Committee 2007. "21 Steps to Improve Cyber Security of SCADA Networks." U.S. Department of Energy. 1 Jan.

Jansen, W. and Grance, T. 2011. *Guidelines on Security and Privacy in Public Cloud Computing.* Draft NIST Special Publication 800-144. Dec.

Janssen, C. 2014. "IT Infrastructure." Technopedia. www.techopedia.com/definition/29199/it-infrastructure. 21 Nov.

Joint Task Force Transformation Initiative 2012. *Security and Privacy Controls for Federal Information Systems and Organizations.* NIST Special Publication 800-53 Revision 4. Feb.

Kaiser, L. 2012. "2013–2023 Transportation Industrial Control Systems Cybersecurity Standards Strategy." U.S. Department of Homeland Security.

Karol, G. 2013. "5 Steps to Recovery After Your Business Has Been Hacked." *FOXBusiness.* smallbusiness.foxbusiness.com/technology-web/2013/02/19/5-steps-to-recovery-afteryour-business-has-been-hacked/. 19 Feb.

Khalaf, S. 2014. "Mobile Use Grows 115% in 2013, Propelled by Messaging Apps." *Flurry from Yahoo.* blog.flurry.com/default.aspx?Tag=Apps. 13 Jan.

Kimery, A. 2014. "Tunisian Hackers Announce Cyber Jihad Against U.S. Banks, Airport Computer Systems." www.hstoday.us. 4 Jul.

Klein, A. 2012. "Man-in-the-Browser: Citadel Trojan Targets Airport Employees with VPN Attack." Blog post. *Trusteer.* 14 Aug.

Kumar, A. 2012. "Airport VPN Hacked Using Citadel Malware." *The Hacker News.* Web. 16 Aug.

Kumar, M. 2011. "Catania airport website hacked, Moroccan Suspected!" *The Hacker News.* Web.

Lofgren, A. 2013. "Practicing Safe BYOD: Is Your Data at Risk?" *All Things D.* Dow Jones & Company Inc. allthingsd.com/20130827/practicing-safe-byod-is-your-data-at-risk/. 27 Aug.

Marfatia, M. 2014. "How Legacy Code Is Exposing Business and Government Systems." *Security Info Watch.* www.securityinfowatch.com/article/11386786/advanced-persistent-threats-plagueapplications-that-were-written-decades-ago-in-deadprogramming-languages. 8 Apr.

Marks, J. 2013. "FAA Considers Putting NextGen Weather System in the Cloud." Nextgov. www.nextgov.com/cloud-computing/2013/02/faa-considers-putting-nextgen-weather-system-cloud/61319/. 14 Feb.

McAfee 2014. "McAfee Labs Threats Report." www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2013.pdf (As of Nov. 15. 2014).

McGraw, G. 2006. *Software Security: Building Security In.* Upper Saddle River, NJ: Addison-Wesley Professional.

Mercedes, K. and Winograd, T. 2008. "Enhancing the Development Life Cycle to Produce Secure Software." Data & Analysis Center for Software. Oct.

Merriam-Webster Dictionary 2014. Encyclopedia Britannica. Inc. www.merriam-webster.com/.

Minneapolis–St. Paul Metropolitan Airports Commission 2014. "Operating Budget." Minnesota.

MITRE Corporation 2014a. "Software Assurance, Making Security Measurable." measurablesecurity.mitre.org/directory/areas/softwareassurance.html (As of Oct.30, 2014).

MITRE Corporation 2014b. CAPEC-1000: Mechanism of Attack, Common Attack Pattern Enumeration and Classification. 7 Nov. capec.mitre.org (Last Viewed May 5, 2015).

MS-ISAC 2014. MS-ISAC Membership Overview.

National Initiative for Cybersecurity Education (NICE) 2014. National Cybersecurity Workforce Framework, Version 1.0, May 2014. National Institute of Standards and Technology. niccs.us-cert.gov/training/national-cybersecurity-workforce-framework.

NIST 2012. *Guide for Conducting Risk Assessments.* NIST Special Publication 800-30 Revision 1. Sept.

NIST 2014. "Framework for Improving Critical Infrastructure Cybersecurity" Version 1, 14 Feb.

Orlando Aviation Authority 2014. "Orlando International Airport and Orlando Executive Airport Budget Fiscal Year 2014–2015." City of Orlando, Florida.

Paganini, P. 2013. "Istanbul Ataturk International Airport Targeted by a Cyber Attack." Securityaffairs.co. 28 Jul.

Palmer, D. 2013. "Education Helps Miami International Airport Reduce Threat of 20,000 Cyber Attacks a Day." *Computing.* www.computing.co.uk/ctg/news/2276385/education-helps-miami-international-airportreduce-threat-of-20-000-cyber-attacks-a-day. 20 Jun.

PCI Security Standards Council 2013. Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures. Version 3.0. Nov.

Peters, G. and Woosley, T. 2009. "The New Sustainable Airport Manual." Presented at Airports Going Green Conference 2009.

Phifer, L. 2013. "BYOD Security Strategies: Balancing BYOD Risks and Rewards." TechTarget SearchSecurity. n.p. searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risksand-rewards. Jan.

Phneah, E. 2013. "BYOD and the Consumerization of IT: Five Security Risks of Moving Data in BYOD Era." *ZDnet.* www.zdnet.com/five-securityrisks-of-moving-data-in-byod-era-7000010665/. 4 Feb.

Port Authority of New York & New Jersey no date. National Alliance to Advance NextGen. www.panynj.gov/airports/nextgen.html (As of Nov. 11, 2014).

Purnell, J., Hough, R., White, R., Gonzalez, S., Haley, F., Hyde, M., Willis, J., de Grandis, G., and Walfish, J. 2012. *ACRP Report 59: Information Technology Systems at Airports—A Primer,* Washington, DC: Transportation Research Board.

Rainie, L., Anderson, J., and Connolly, J. 2014. "Cyber Attacks Likely to Increase." *Pew Research Internet Project.* Pew Research Center. www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/. 29 Oct.

Ranasinghe, D. 2014. "Technology the Backbone of World's Best Airport" *TechEdge, A CNBC Special Report.* www.cnbc.com/id/101521255#. 30 Mar.

Razo, J. R. 2012. "Overview of Best Practices for Protecting Sensitive Information." Presented at Dartmouth College's Securing the eCampus 2012 Conference, July 17. www.ists.dartmouth.edu/docs/ecampus/2012/2012ecampus_razo.pdf.

Rios, B. 2014. "Pulling the Curtain on Airport Security." Presented at the BlackHat 2014 Conference.

Roadmap to Secure Control Systems in the Transportation Sector Working Group 2012. "Roadmap to Secure Control Systems in the Transportation Sector." Control Systems Security Program, National Cybersecurity Division, U.S. Department of Homeland Security. Aug.

Rouse, M. 2011. "Endpoint Security." *TechTarget.* Web. Jun.

Sawyer, R. 2007. *The Seven Military Classics of Ancient China.* New York: Basic Books.

Selvan, S. 2013. "Dubai International Hacked by Portugal Cyber Army." *E Hacking News.* Web. 19 Apr. 2013.

Silowash, G., Cappelli, D., Moore, A. P., Trzeciak, R. F., Shimeall, T. J., and Flynn, L. 2012. *Common Sense Guide to Mitigating Insider Threats,* 4th Edition. Software Engineering Institute, December.

Software Assurance Marketplace 2014. Currently Available Open Source Assurance Tools. Morgridge Institute for Research. continuousassurance.org/solutions/tool-selection/ (As of Oct. 30, 2014).

Souppaya, M. and Scarfone, K. 2013. *Guidelines for Managing the Security of Mobile Devices in the Enterprise.* NIST Special Publication 800-124 Revision 1.

Stapleton, T. 2014. "Human Error: The Biggest Cyber Security Threat?" *Strategic Risk.* n.p. www.strategic-riskglobal.com/human-error-the-biggest-cyber-securitythreat/1410557.article. 30 Oct.

Stotts, R. and Lippenholz, S. 2014. "Cyber Hunting: Proactively Track Anomalies to Inform Risk Decisions." Booz Allen Hamilton. www.boozallen.com/insights/2013/03/cyber-hunting-proactively-track-anomalies-to-inform-risk-decisions (As of Oct. 22, 2014).

Stouffer, K., Falco, J., and Scarfone, K. 2013. *Guide to Industrial Control Systems Security.* NIST Special Publication 800-82, Revision 1. May.

Strahler, S. 2014. "A New Job Title for 2014: CISO." *Crain's Chicago Business.* www.chicagobusiness.com/article/20140913/ISSUE02/309139997/a-new-job-title-for-2014-ciso. 15 Sept.

Sullivan, A. 2013. "Obama Budget Makes Cybersecurity a Growing U.S. Priority." Reuters. 10 Apr.

Transportation Security Administration 2014. Security Technologies. www.tsa.gov/about-tsa/security-technologies (As of October 30, 2014).

U.S. Department of Energy 2008. "Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program." Office of Electricity Delivery and Energy Reliability. Nov.

U.S. Department of Energy 2014. "National SCADA Test Bed Fact Sheet, Office of Electricity Delivery and Energy Reliability." energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf (Last Viewed Nov. 21, 2014).

U.S. Department of Homeland Security 2009. "Cyber Security Procurement Language for Control Systems." Control Systems Security Program, National Cyber Security Division. Sept.

U.S. Department of Homeland Security 2010. "Cyber Security Assessments of Industrial Control Systems." ics-cert.uscert.gov/sites/default/files/documents/Cyber_Security_Assessments_of_Industrial_Control_Systems.pdf. Nov.

U.S. Department of Homeland Security 2012. "Federal Continuity Directive 1." Oct.

Verizon 2012. Verizon Enterprise Risk and Incident Sharing Metrics Framework. White paper.

Verizon 2014. "Verizon 2014 PCI Compliance Report." www.verizonenterprise.com/pcireport/2014/ (As of June 16, 2014).

Vijay 2014. "Airports Authority of India (AAI) Hacked, Critical Data Compromised." *TechWorm.* www.techworm.net/2014/09/airports-authority-of-india-hacked.html. 24 Sept.

White House 2009. "Cyberspace Policy Review." www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Wi-Fi Alliance 2015. Discover Wi-Fi: Security. http://www.wi-fi.org/discover-wi-fi/security (Last Viewed May 5, 2015).

APPENDIX A

Categorized List of Cybersecurity Threats

Following is a categorized list of threats that may affect airport data and systems.

Category	Name	Description
Confidentiality Breach	Compromise of encryption material	Adversary able to gain access to encryption keys.
	Release of personally identifiable information (PII)	Intentional or unintentional release of PII.
Counterfeit Hardware	Compromise of 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.
	Counterfeit or tampered-with hardware into the supply chain	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.
Data Breach	Compromise of 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.
Delayed Technology Refresh	Resource depletion	Degraded processing performance due to resource depletion.
	Unreadable display	Display unreadable due to aging equipment.
Denial of Service (DoS)	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.
	Simple 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.
	Targeted DoS attacks	Adversary targets DoS attacks to critical information systems, components, or supporting infrastructures, based on adversary knowledge of dependencies.
Host 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.
	Wireless jamming attacks	Adversary takes measures to interfere with wireless communications so as to impede or prevent communications from reaching intended recipients.
Inadequate Monitoring of Proximity Events	Events occurring to any critical infrastructure near the airport like railroad, subway, or chemical storage	Failure to monitor any events in the proximity of an airport that may cause indirect damage or disruption in airport services.
Ineffective Disposal	Obtaining 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.

Category	Name	Description
Ineffective Testing	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.
	Reverse engineering	An attacker discovers the structure, function, and composition of an object, resource, or system by using a variety of analysis techniques to effectively determine how the analyzed entity was constructed or operates. The goal of reverse engineering is often to duplicate the function, or a part of the function, of an object in order to duplicate or "back engineer" some aspect of its functioning. Reverse engineering techniques can be applied to mechanical objects, electronic devices or components, or to software, although the methodology and techniques involved in each type of analysis differ widely.
	Software integrity attacks	An attacker initiates a series of events designed to cause a user, program, server, or device to perform actions which undermine the integrity of software code, device data structures, or device firmware, achieving the modification of the target's integrity to achieve an insecure state.
	Software reverse engineering	An attacker discovers the structure, function, and composition of a type of computer software by using a variety of analysis techniques to effectively determine how the software functions and operates or if vulnerabilities or security weaknesses are present within the implementation. Reverse engineering methods, as applied to software, can utilize a wide number of approaches and techniques.
Insider Threat	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 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 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.
	Insert of 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 of 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.
	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).
	Vulnerabilities exploited by leveraging internal organizational information systems	Adversary searches for known vulnerabilities in organizational internal information systems and exploits those vulnerabilities.

(continued on next page)

Category	Name	Description
Insider Threat / Data Breach	Compromise of 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.
	Vulnerabilities exploited 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.
Intentional Data Alteration	Data 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.
	Data 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.
	Data 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.
Intentional Data Theft	Gaining access to sensitive information via exfiltration	Adversary directs malware on organizational systems to locate and surreptitiously transmit sensitive information.
Internal Threat	Robbery	This relates to the act or an instance of unlawfully taking the property of another by the use of violence or intimidation.
Lack of Internal Control	Insecure or incomplete data deletion in multi-tenant environment	Adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment (e.g., in a cloud computing environment).
Malicious Code	Application API message manipulation via man-in-the-middle (MITM)	An attacker manipulates either egress or ingress data from a client within an application framework in order to change the content of messages. Performing this attack can allow the attacker to gain unauthorized privileges within the application, or conduct attacks such as phishing, deceptive strategies to spread malware, or traditional web-application attacks. The techniques require use of specialized software that allows the attacker to intercept communications between the web browser and the remote system (i.e., “man-in-the-middle” attack). Despite the use of MITM software, the attack is actually directed at the server, as the client is one node in a series of content brokers that pass information along to the application framework. Additionally, it is not true MITM attack at the network layer, but an application-layer attack, the root cause of which is the master application’s trust in the integrity of code supplied by the client.
	Compromise of critical information systems via physical access	Adversary obtains physical access to organizational information systems and makes modifications.
	Compromise of 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.
	Insert specialized malicious code 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.

Category	Name	Description
Malicious Code (Continued)	Malicious code delivery 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.
	Malware injection using provided 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).
	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.
	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.
	Targeted malware injection 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).
	Targeted malware to take control of internal systems and exfiltrate 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.
	Untargeted malware injection 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.
Organized 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 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.
Phishing	Creating and operating 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.
	Other phishing attacks	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or Social Security numbers. 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.
	Spear phishing attacks	Adversary employs phishing attacks targeted at high-value targets (e.g., senior leaders/executives).
Physical Exploit	Cyber–physical attacks on organizational facilities	Adversary conducts a cyber–physical attack on organizational facilities (e.g., remotely changes HVAC settings).

(continued on next page)

Category	Name	Description
Social Engineering	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.
	Compromise of 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.
	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., PII).
Supply Chain Integrity	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 perform critical functions for organizations. This is largely accomplished as supply-chain attacks on both commercial off-the-shelf and custom information systems and components.
Third Party	Pervasive disk error	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.
Unauthorized Access (host, network or app)	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, smartphones). The intent is to take advantage of any instances where employees use personal information systems or devices to handle critical/sensitive information.
	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.
	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.
	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.
	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 function.
	Data-scavenging attacks in a cloud environment	Adversary obtains data used and then deleted by organizational processes running in a cloud environment.
	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.
	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.

Category	Name	Description
Unauthorized Access (host, network or app) (Continued)	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.
	Internally based network traffic modification (man-in-the-middle) attacks	Adversary operating within the organizational infrastructure intercepts and corrupts data sessions.
	Tampered-with critical components into organizational systems	Adversary replaces, through supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.
Unauthorized Back Door	Obfuscate adversary actions	Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations.
Unauthorized Host Access	Compromise of software of critical organizational information systems	Adversary inserts malware or otherwise corrupts critical internal organizational information systems.
	Counterfeit certificates	Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.
	Creating counterfeit/spoof website	Adversary creates duplicates of legitimate websites; when users visit a counterfeit site, the site can gather information or download malware.
Unauthorized Network Access	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.
	Breaking into an isolated 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.
	Exploitation of 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 non-secure remote connect.
	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).
	General-purpose sniffers on organization-controlled information systems or networks	Adversary installs sniffing software onto internal organizational information systems or networks.
	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) of 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.
	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.

(continued on next page)

Category	Name	Description
Unauthorized Network Access (Continued)	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.
	Obtaining 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.
	Persistent and targeted sniffers installed 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.
Unauthorized Physical Access	Bypassing card- or badge-based systems	An attacker bypasses the security of a card-based system by using techniques such as cloning access cards or using brute-force techniques. Card-based systems are widespread throughout business, government, and supply-chain management. Attacks against card-based systems vary widely based on the attackers' goals but commonly include unauthorized reproduction of cards, brute-force creation of valid card-values, and attacks against systems which read or process card data. Due to the inherent weaknesses of card and badge security, high-security environments will rarely rely upon the card or badge alone as a security mechanism. Common card-based systems are used for financial transactions, user identification, and access control. Cloning attacks involve making an unauthorized copy of a user's card while brute-force attacks involve creating new cards with valid values. Denial of service attacks against card-based systems involve rendering the reader, or the card itself, disabled. Such attacks may be useful in a fail-closed system for keeping authorized users out of a location while a crime is in progress, whereas fail-open systems may grant access, or an alarm may fail to trigger, if an attacker disables or damages the card authentication device.
	Cloning magnetic strip cards	An attacker duplicates the data on a magnetic strip card (i.e., "swipe card" or "magstripe") to gain unauthorized access to a physical location or a person's private information. Magstripe cards encode data on a band of iron-based magnetic particles arrayed in a stripe along a rectangular card. Most magstripe card data formats conform to ISO standards 7810, 7811, 7813, 8583, and 4909. The primary advantage of magstripe technology is ease of encoding and portability, but this also renders magnetic strip cards susceptible to unauthorized duplication. If magstripe cards are used for access control, all an attacker need do is obtain a valid card long enough to make a copy of the card and then return the card to its location (i.e., a co-worker's desk). Magstripe reader/writers are widely available as well as software for analyzing data encoded on the cards. By swiping a valid card, it becomes trivial to make any number of duplicates that function as the original.

Category	Name	Description
Unauthorized Physical Access (Continued)	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).
	Physical attacks on organizational facilities	Adversary conducts a physical attack on organizational facilities (e.g., sets a fire).
Unauthorized Reconnaissance	Access to 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.
	Cyberattacks based on detailed surveillance	Adversary adapts behavior in response to surveillance and organizational security measures.
	Gathering 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.
	Information gathering using open-source discovery of organizational information	Adversary mines publicly 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.
	Internal malware-directed 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.
	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.
	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.
Unintended Data Compromise	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.
	Mishandling of critical and/or sensitive information by authorized users	Authorized privileged user inadvertently exposes critical/sensitive information.
	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 to access such information, and the information system, device, or network is unavailable while the spill is investigated and mitigated.
Unintended Data Leak	Incorrect privilege settings	Authorized privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low.

(continued on next page)

Category	Name	Description
Unintended Data Leak (Continued)	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.
Unpatched Hosts	Exploitation of known vulnerabilities in mobile systems (e.g., laptops, PDAs, smartphones)	Adversary takes advantage of transportable information systems being outside the physical protection of organizations and the logical protection of corporate firewalls, and compromises the systems based on known vulnerabilities to gather information from those systems.
	Exploitation of 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.
Vishing	Compromise or gaining access to critical information systems	Using voice systems as social engineering technique to break, compromise, or gain access to critical information systems.

Source: NIST (2012), Verizon (2012), MITRE Corporation (2014b), and research team experience.

APPENDIX B

Airport Systems

Following is a categorized list of the types of systems often found at airports.

Type	Name
Administration Systems	Airport Revenue Management
	Airport Staff Rostering
	Asset Inventory Management System
	Audio Management Systems
	Cable Locations and Asset Management
	CNN News TV Monitor
	Database Management Systems
	Documentation Management Systems
	Drawings Management Systems
	E-Commerce Website for Airport and Tenants
	E-Mail Management Systems
	Enterprise Content Management System (ECMS)
	Financial Assets
	Financial Management System
	Graphics/Photos Management Systems
	Human Resources Management System
	Insurances and Benefits Management
	Intellectual Property Assets
	IT Assets
	Library and Regulation Management
	Meeting Management (Events Scheduling)
	Noise Monitoring Systems
	Payroll
	Procurement Management System
	Property Management System
	Public Addressing
	Recruitment Management Systems
	Space & Lease Management System
	Spatial Database
	Staff Records Management
	Tenant Relations – Billing Administration
	Tenant Relations – Business Services

(continued on next page)

Type	Name
Administration Systems (Continued)	Tenant Relations – Contract/Lease Administration
	Tenant Relations – Electronic Bill Payment
	Tenant Relations – Point of Sale & Revenue Management Systems
	Tenant Relations – Product Catalog Management
	Tenant Relations – Product Provisioning
	Time and Attendance
	Tourism and Hotel Information
	Video Management Systems
Airline & Airside Operations Systems	Advertising Information Display Systems
	Aircraft Refueling Systems
	Aircraft Servicing
	Airfield Lighting Control System
	Airline Gateway Server Systems
	Airport Operational Database (AODB)
	Apron and Air Bridge Operation
	Baggage Carousel Management System
	Baggage Handling Systems (BHS)
	Baggage Information Display Systems (BIDS)
	Baggage Reconciliation System
	Baggage Sortation System
	Baggage Tracking System
	Cargo Processing Systems
	Common Language Facility (CLF – translations for Ground Handlers' scripts)
	Common Use Passenger Processing Systems (CUPPS)
	Common Use Self-Service (CUSS) Kiosks
	Common Use Terminal Equipment (CUTE)
	Daily Operations Log and Emergency Checklists
	De-icing Systems
	Departure Control Systems (DCS)
	Electronic Visual Information Display Systems (EVIDS)
	FAA Air Traffic Control & Navigational Aids & Approach Lighting Systems
	Flight Information Display Systems (FIDS)
	Flight Tracking Systems
	Gate Information Display System (GIDS)
	Gate Management System
	Local DCS & Weight and Balance
	Meteorological Information
	Noise Monitoring Systems
	Parking Information Display Systems
	Passenger Check-in and Boarding
	Passenger Loading Bridge Systems
	Ramp Information Display Systems (RIDS)
	Resource Management System (RMS)

Type	Name
Airline & Airside Operations Systems (Continued)	Runway Lighting
	Runway Monitoring System
	Self-Service Kiosks (CUSS)
	Ticket Counter Management System
	Transportation Information
	Tug Drive Information System
	ULD & LD3 – Unit Load Device Tracking
	Visual Docking Guidance System
	Visual Paging & Emergency Display Systems
	Visual Passenger Information Systems
	Wayfinding Information Display Systems
	Weather Tracking Systems (AWOS)
Cloud-Based Services	Our Applications in the Cloud
	Our Data in the Cloud
Development Systems	Airspace & NAVAID Obstruction Management System
	Certification Laboratory (for applications and hardware under consideration)
	Circulation Flow Analysis & Simulation System
	Computer Aided Design & Drafting (CADD)
	Drawing Management System
	Environmental Management System
	Geographic Information System (GIS)
	Marketing
	Marketing – Advertising Decision-Making Systems
	Marketing – Business Intelligence Support
	Marketing – Community Outreach Support
	Marketing – Passenger Outreach Support
	Marketing – Tenant Outreach Support
	Pavement Management System
	Project Management System
	Three-Dimensional Visualization System
Employee Devices	Employee Handheld Devices
	Employee Workstations
Facilities & Maintenance Systems	Air Bridge Maintenance
	Airport Vehicle Maintenance
	Building Control Systems
	Computerized Maintenance Management System (CMMS)
	Electric Power
	Elevators
	Energy Management
	Escalators
	HVAC
	Light Rail
	Lighting

(continued on next page)

Type	Name
Facilities & Maintenance Systems (Continued)	Maintenance and Construction Management
	Material Management
	Moving Walkways
	People Mover Systems
	Sewage Processing
	Signage Management System
	Storm Water Run-off
	Supervisory Control and Data Acquisition (SCADA)
	Turnstiles
	Utilities Metering Systems
	Vehicle Parking Access Maintenance
	Waste Burning Management
	Waste Management
IT & Communications Systems	ACARS Messaging
	AFTN Messaging (including FAA & ATC)
	Cable Management System
	Cellular Telephone
	Communication Systems
	Data Center and Associated Hardware
	Ethernet
	Extranet
	FAA Messaging
	Gateways
	IATA Messaging (Type-B)
	Integrated 800 MHz Trunked Radio, Land Mobile Radio, TETRA, etc.
	Interfaces to IT Help Desk
	Internet
	Intranet
	Local Area Network (LAN)
	Master Clock
	Multi-frequency Antennae
	Network Security Management
	Network Systems
	Passive Infrastructure
	Premises Distribution (Wiring & Backbone) Systems
	Private Branch Exchange (PBX) Telephone
	Radio Spectrum Management Systems
	Virtual Private Networks (VPN)
	VoIP Telephone
	VoWiFi Telephone
	Web Gateways
	Wide Area Network (WAN)
	Wi-Fi
	Wireless Access Points

Type	Name
Landside Operations Systems	Airport Landside Operations Systems Control Center
	Automated Vehicle Identification (AVI)
	Electronic Parking Toll (e.g., E-Pass)
	Fuel Chargebacks
	Fuel Management
	Fuel Reordering and Monitoring of Fuel Levels
	License Tag Identification System
	Lightning Detection Systems
	Parking Revenue Control
	Parking Space Management System
	Parking Systems
	Surface Vehicle Monitoring System
	Taxi Dispatch System
Safety & Security Systems	Access Control
	Access Control Systems
	APIS – for inbound, international flights
	Badging Systems
	Baggage Screening Systems – EDS
	Biometrics Systems
	Camera Systems
	Closed Circuit Television (CCTV)
	Command & Control Center Systems
	Computer Aided Dispatch (CAD)
	Customs/Immigration
	e911
	Emergency Response System
	Fire Fighting & Alarm Systems
	In-Line Explosives Detection Systems (EDS)
	Mobile Command Post Systems
	Natural Disaster Operation
	Passenger Screening Systems
	Perimeter Intrusion Detection Systems (PIDS)
	Perimeter Security
	Screening Systems (Passenger Carry-on Baggage)
	US Visit Systems
	Video Surveillance
	Voice Communications
Tenant Systems	Automatic Teller Machines
	Point-of-Sales Machines
	Tenant Point-of-Sale Devices

Source: Airport Consultants Council (2012); results from survey conducted for this project.

APPENDIX C

Countermeasures

Following is a categorized and prioritized list of countermeasures that airports should consider when addressing vulnerabilities to reduce their likelihood of a successful cybersecurity attack. References refer to NIST 800-53 (Joint Task Force Transformation Initiative 2012) where additional information on each countermeasure can be found.

Ref	Class	Type	Name	Priority	Description	Guidance
PL-1	Management	Planning	Security Planning Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security planning policy. Related control: PM-9.
PL-2	Management	Planning	System Security Plan	P1	The organization: a. Develops a security plan for the information system that: - Is consistent with the organization's enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context of the information system in terms of missions and business processes; - Provides the security categorization of the information system including supporting rationale; - Describes the operational environment for the information system; - Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system [Assignment: organization-defined frequency]; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.	The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Related controls: PM-1, PM-7, PM-8, PM-9, PM-11.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
PL-4	Management	Planning	Rules of Behavior	P1	The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behavior. Related control: PS-6.
PL-5	Management	Planning	Privacy Impact Assessment	P1	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	None.
PL-6	Management	Planning	Security-Related Activity Planning	P3	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.	Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises. Organizational advance planning and coordination includes both emergency and nonemergency (i.e., planned or nonurgent unplanned) situations.
PM-1	Management	Program Management	Information Security Program Plan	P1	The organization: a. Develops and disseminates an organization-wide information security program plan that: - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; - Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; - Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; - Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [Assignment: organization-defined frequency]; and c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.	The information security program plan can be represented in a single document or compilation of documents at the discretion of the organization. The plan documents the organization-wide program management controls and organization-defined common controls. The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls. Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems. Related control: PM-8.

Ref	Class	Type	Name	Priority	Description	Guidance
PM-2	Management	Program Management	Senior Information Security Officer	P1	The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this organizational official as the Senior Information Security Officer or Chief Information Security Officer.
PM-3	Management	Program Management	Information Security Resources	P1	The organization: a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.	Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process. Related controls: PM-4, SA-2.
PM-4	Management	Program Management	Plan of Action and Milestones Process	P1	The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.	The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. Related control: CA-5.
PM-5	Management	Program Management	Information System Inventory	P1	The organization develops and maintains an inventory of its information systems.	This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements.
PM-6	Management	Program Management	Information Security Measures of Performance	P1	The organization develops, monitors, and reports on the results of information security measures of performance.	Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.
PM-7	Management	Program Management	Enterprise Architecture	P1	The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This also embeds into the enterprise architecture, an integral security architecture consistent with organizational risk management and information security strategies. Security requirements and control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures. Related controls: PL-2, PM-11, RA-2.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
PM-8	Management	Program Management	Critical Infrastructure Plan	P1	The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: PM-1, PM-9, PM-11, RA-3.
PM-9	Management	Program Management	Risk Management Strategy	P1	The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and b. Implements that strategy consistently across the organization.	An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive. Related control: RA-3.
PM-10	Management	Program Management	Security Authorization Process	P1	The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program.	The security authorization process for information systems requires the implementation of the Risk Management Framework and the employment of associated security standards and guidelines. Specific roles within the risk management process include a designated authorizing official for each organizational information system. Related control: CA-6.
PM-11	Management	Program Management	Mission/Business Process Definition	P1	The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. Related controls: PM-7, PM-8, RA-2.

Ref	Class	Type	Name	Priority	Description	Guidance
RA-1	Management	Risk Assessment	Risk Assessment Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the risk assessment family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the risk assessment policy. Related control: PM-9.
RA-2	Management	Risk Assessment	Security Categorization	P1	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability. The organization conducts the security categorization process as an organization-wide activity with the involvement of the chief information officer, senior information security officer, information system owner, mission owners, and information owners/stewards. The organization also considers potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts in categorizing the information system. The security categorization process facilitates the creation of an inventory of information assets, and in conjunction with CM-8, a mapping to the information system components where the information is processed, stored, and transmitted. Related controls: CM-8, MP-4, SC-7.
RA-3	Management	Risk Assessment	Risk Assessment	P1	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; c. Reviews risk assessment results [Assignment: organization-defined frequency]; and d. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	A clearly defined authorization boundary is a prerequisite for an effective risk assessment. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to organizational operations and assets, individuals, other organizations, and the Nation based on the operation of the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
						nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems. Risk assessments (either formal or informal) can be conducted by organizations at various steps in the Risk Management Framework including: information system categorization; security control selection; security control implementation; security control assessment; information system authorization; and security control monitoring. RA-3 is a noteworthy security control in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the tailored baselines with additional security controls or control enhancements.
RA-5	Management	Risk Assessment	Vulnerability Scanning	P1	The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and - Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers). Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms. The organization considers using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities. The Common Weakness Enumeration (CWE) and the National Vulnerability Database (NVD) are also excellent sources for vulnerability information. In addition, security control assessments such as red team exercises are another source of potential vulnerabilities for which to scan. Related controls: CA-2, CM-6, RA-3, SI-2.
CA-1	Management	Security Assessment & Authorization	Security Assessment and Authorization Policies and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security assessment and authorization family. The policies and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and

Ref	Class	Type	Name	Priority	Description	Guidance
					b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security assessment/authorization policies can be included as part of the general information security policy for the organization. Security assessment/authorization procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security assessment and authorization policy. Related control: PM-9.
CA-2	Management	Security Assessment & Authorization	Security Assessments	P2	The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be used to determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.	The organization assesses the security controls in an information system as part of: (i) security authorization or reauthorization; (ii) meeting the FISMA requirement for annual assessments; (iii) continuous monitoring; and (iv) testing/evaluation of the information system as part of the system development life cycle process. The assessment report documents the assessment results in sufficient detail as deemed necessary by the organization, to determine the accuracy and completeness of the report and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the information system. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security authorization process. To satisfy the FISMA annual assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) assessments conducted as part of an information system authorization or reauthorization process; (ii) continuous monitoring (see CA-7); or (iii) testing and evaluation of an information system as part of the ongoing system development life cycle (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security control assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Subsequent to the initial authorization of the information system and in accordance with OMB policy, the organization assesses a subset of the security controls annually during continuous monitoring. The organization establishes the security control selection criteria and subsequently selects a subset of the security controls within the information system and its environment of operation for assessment. Those security controls that are the most volatile (i.e., controls most affected by ongoing changes to the information system or its environment of operation) or deemed critical by the organization to

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
						protecting organizational operations and assets, individuals, other organizations, and the Nation are assessed more frequently in accordance with an organizational assessment of risk. All other controls are assessed at least once during the information system's three-year authorization cycle. The organization can use the current year's assessment results from any of the above sources to meet the FISMA annual assessment requirement provided that the results are current, valid, and relevant to determining security control effectiveness. External audits (e.g., audits conducted by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-6, CA-7, PM-9, SA-11.
CA-3	Management	Security Assessment & Authorization	Information System Connections	P1	The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.	This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing. The organization carefully considers the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within the organization and external to the organization. Authorizing officials determine the risk associated with each connection and the appropriate controls employed. If the interconnecting systems have the same authorizing official, an Interconnection Security Agreement is not required. Rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems. If the interconnecting systems have different authorizing officials but the authorizing officials are in the same organization, the organization determines whether an Interconnection Security Agreement is required, or alternatively, the interface characteristics between systems are described in the security plans of the respective systems. Instead of developing an Interconnection Security Agreement, organizations may choose to incorporate this information into a formal contract, especially if the interconnection is to be established between a federal agency and a nonfederal (private sector) organization. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the information systems. Risk considerations also include information systems sharing the same networks. Information systems may be identified and authenticated as devices in accordance with IA-3. Related controls: AC-4, IA-3, SC-7, SA-9.
CA-5	Management	Security Assessment & Authorization	Plan of Action and Milestones	P3	The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and	The plan of action and milestones is a key document in the security authorization package and is subject to federal reporting requirements established by OMB. Related control: PM-4.

Ref	Class	Type	Name	Priority	Description	Guidance
					b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	
CA-6	Management	Security Assessment & Authorization	Security Authorization	P3	The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [Assignment: organization-defined frequency].	Security authorization is the official management decision, conveyed through the authorization decision document, given by a senior organizational official or executive (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. Authorizing officials typically have budgetary oversight for information systems or are responsible for the mission or business operations supported by the systems. Security authorization is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials are accountable for the security risks associated with information system operations. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report, and the plan of action and milestones) is updated on an ongoing basis, providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative cost of security reauthorization, the authorizing official uses the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision. OMB policy requires that federal information systems are reauthorized at least every three years or when there is a significant change to the system. The organization defines what constitutes a significant change to the information system. Related controls: CA-2, CA-7, PM-9, PM-10.
CA-7	Management	Security Assessment & Authorization	Continuous Monitoring	P3	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials [Assignment: organization-defined frequency].	A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system. The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones, the three principal documents

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
						in the security authorization package. A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the security categorization of the information system. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4.
SA-1	Management	System & Services Acquisition	System and Services Acquisition Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and services acquisition family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and services acquisition policy. Related control: PM-9.
SA-2	Management	System & Services Acquisition	Allocation of Resources	P1	The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.	Related controls: PM-3, PM-11.
SA-3	Management	System & Services Acquisition	Life Cycle Support	P1	The organization: a. Manages the information system using a system development life cycle methodology that includes information security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities.	Related control: PM-7.
SA-4	Management	System & Services Acquisition	Acquisitions	P1	The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements.	The acquisition documents for information systems, information system components, and information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the acquisition documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. Acquisition documents also include requirements for appropriate information system documentation. The documentation addresses

Ref	Class	Type	Name	Priority	Description	Guidance
						user and system administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the security categorization for the information system. In addition, the required documentation includes security configuration settings and security implementation guidance. FISMA reporting instructions provide guidance on configuration requirements for federal information systems.
SA-5	Management	System & Services Acquisition	Information System Documentation	P2	The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes: - User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and - User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.	The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.
SA-6	Management	System & Services Acquisition	Software Usage Restrictions	P1	The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.
SA-7	Management	System & Services Acquisition	User-Installed Software	P1	The organization enforces explicit rules governing the installation of software by users.	If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect). Related control: CM-2.
SA-8	Management	System & Services Acquisition	Security Engineering Principles	P1	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
						system. Examples of security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring system developers and integrators are trained on how to develop secure software; (vi) tailoring security controls to meet organizational and operational needs; and (vii) reducing risk to acceptable levels, thus enabling informed risk management decisions.
SA-9	Management	System & Services Acquisition	External Information System Services	P1	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers.	An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The extent and nature of this chain of trust varies based on the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.
SA-10	Management	System & Services Acquisition	Developer Configuration Management	P1	The organization requires that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation; b. Manage and control changes to the information system; c. Implement only organization-approved changes; d. Document approved changes to the information system; and e. Track security flaws and flaw resolution.	Related controls: CM-3, CM-4, CM-9.

Ref	Class	Type	Name	Priority	Description	Guidance
SA-11	Management	System & Services Acquisition	Developer Security Testing	P2	The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security test and evaluation plan; b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and c. Document the results of the security testing/evaluation and flaw remediation processes.	Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system. Related control: CA-2, SI-2.
SA-12	Management	System & Services Acquisition	Supply Chain Protection	P1	The organization protects against supply chain threats by employing: [Assignment: organization-defined list of measures to protect against supply chain threats] as part of a comprehensive, defense-in-breadth information security strategy.	A defense-in-breadth approach helps to protect information systems (including the information technology (IT) products that compose those systems) throughout the system development life cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk.
SA-13	Management	System & Services Acquisition	Trustworthiness	P1	The organization requires that the information system meets [Assignment: organization-defined level of trustworthiness].	The intent of this control is to ensure that organizations recognize the importance of trustworthiness and making explicit trustworthiness decisions when designing, developing, and implementing organizational information systems. Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of risk despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Two factors affecting the trustworthiness of an information system include: (i) security functionality (i.e., the security features or functions employed within the system); and (ii) security assurance (i.e., the grounds for confidence that the security functionality is effective in its application). Appropriate security functionality for the information system can be obtained by using the Risk Management Framework (Steps 1, 2, and 3) to select and implement the necessary management, operational, and technical security controls necessary to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Appropriate security assurance can be obtained by: (i) the actions taken by developers and implementers of security controls with regard to the design, development, implementation, and operation of those controls; and (ii) the actions taken by assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
						Developers and implementers can increase the assurance in security controls by employing well-defined security policy models, structured, disciplined, and rigorous hardware and software development techniques, and sound system/security engineering principles. Assurance is also based on the assessment of evidence produced during the initiation, acquisition/development, implementation, and operations/maintenance phases of the system development life cycle. For example, developmental evidence may include the techniques and methods used to design and develop security functionality. Operational evidence may include flaw reporting and remediation, the results of security incident reporting, and the results of the ongoing monitoring of security controls. Independent assessments by qualified assessors may include analyses of the evidence as well as testing, inspections, and audits. Explicit trustworthiness decisions highlight situations where achieving the information system resilience and security capability necessary to withstand cyberattacks from adversaries with certain threat capabilities may require adjusting the risk management strategy, the design of mission/business processes with regard to automation, the selection and implementation rigor of management and operational protections, or the selection of IT components with higher levels of trustworthiness. Trustworthiness may be defined on a component-by-component, subsystem-by-subsystem, or function-by-function basis. It is noted, however, that typically functions, subsystems, and components are highly interrelated, making separation by trustworthiness perhaps problematic and at a minimum, something that likely requires careful attention in order to achieve practically useful results. Related controls: RA-2, SA-4, SA-8, SC-3.
SA-14	Management	System & Services Acquisition	Critical Information System Components	P0	The organization: a. Determines [Assignment: organization-defined list of critical information system components that require re-implementation]; and b. Re-implements or custom develops such information system components.	The underlying assumption is that the list of IT products defined by the organization cannot be trusted due to threats from the supply chain that the organization finds unacceptable. The organization re-implements or custom develops such components to satisfy requirements for high assurance. Related controls: SA-12, SA-13.
AT-1	Operational	Awareness & Training	Security Awareness and Training Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security awareness and training family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security awareness and training policy. Related control: PM-9.

Ref	Class	Type	Name	Priority	Description	Guidance
AT-2	Operational	Awareness & Training	Security Awareness	P1	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [Assignment: organization-defined frequency] thereafter.	The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific requirements of the organization and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security as it relates to the organization's information security program. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.
AT-3	Operational	Awareness & Training	Security Training	P1	The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [Assignment: organization-defined frequency] thereafter.	The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of the organization's information security program. Related controls: AT-2, SA-3.
AT-4	Operational	Awareness & Training	Security Training Records	P3	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [Assignment: organization-defined time period].	While an organization may deem that organizationally mandated individual training programs and the development of individual training plans are necessary, this control does not mandate either. Documentation for specialized training may be maintained by individual supervisors at the option of the organization.
AT-5	Operational	Awareness & Training	Contacts With Security Groups and Associations	P0	The organization establishes and institutionalizes contact with selected groups and associations in the US and internationally, within the security community: - To facilitate ongoing security education and training for organizational personnel; - To stay up to date with the latest recommended security practices, techniques, and technologies; and - To share current security-related information including threats, vulnerabilities, and incidents.	Ongoing contact with security groups and associations is of paramount importance in an environment of rapid technology changes and dynamic threats. Security groups and associations can include, for example, special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. The groups and associations selected are consistent with the organization's mission/business requirements. Information-sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
CM-1	Operational	Configuration Management	Configuration Management Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the configuration management family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the configuration management policy. Related control: PM-9.
CM-2	Operational	Configuration Management	Baseline Configuration	P1	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture. The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. The baseline configuration of the information system is consistent with the organization's enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9.
CM-3	Operational	Configuration Management	Configuration Change Control	P1	The organization: a. Determines the types of changes to the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection: (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].	The organization determines the types of changes to the information system that are configuration controlled. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to components of the information system, changes to the configuration settings for IT products (e.g., operating systems, applications, firewalls, routers), emergency changes, and changes to remediate flaws. A typical organizational process for managing configuration changes to the information system includes, for example, a chartered Configuration Control Board that approves proposed changes to the system. Auditing of changes refers to changes in activity before and after a change is made to the information system and the auditing activities required to implement the change. Related controls: CM-4, CM-5, CM-6, SI-2.

Ref	Class	Type	Name	Priority	Description	Guidance
CM-4	Operational	Configuration Management	Security Impact Analysis	P2	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	Security impact analyses are conducted by organizational personnel with information security responsibilities, including for example, Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers. Individuals conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the security categorization of the information system. Related controls: CA-2, CA-7, CM-3, CM-9, SI-2.
CM-5	Operational	Configuration Management	Access Restrictions for Change	P1	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries. Examples of access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the information system component), and change windows (e.g., changes occur only during specified times, making unauthorized changes outside the window easy to discover). Some or all of the enforcement mechanisms and processes necessary to implement this security control are included in other controls. For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the information system, auditing changes, and retaining and review records of changes. Related controls: AC-3, AC-6, PE-3.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
CM-6	Operational	Configuration Management	Configuration Settings	P1	The organization: a. Establishes and documents mandatory configuration settings for IT products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	Configuration settings are the configurable security-related parameters of IT products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections. Organizations establish organization-wide mandatory configuration settings from which the settings for a given information system are derived. A security configuration checklist (sometimes referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide [STIG], or benchmark) is a series of instructions or procedures for configuring an information system component to meet operational requirements. Checklists can be developed by IT developers and vendors, consortia, academia, industry, federal agencies (and other government organizations), and others in the public and private sectors. An example of a security configuration checklist is the Federal Desktop Core Configuration (FDCC) which potentially affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Related controls: CM-2, CM-3, SI-4.
CM-7	Operational	Configuration Management	Least Functionality	P1	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services].	Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by organizational information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, file sharing). Organizations consider disabling unused or unnecessary physical and logical ports and protocols (e.g., Universal Serial Bus [USB], File Transfer Protocol [FTP], Internet Protocol Version 6 [IPv6], Hyper Text Transfer Protocol [HTTP]) on information system components to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools,

Ref	Class	Type	Name	Priority	Description	Guidance
						intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related control: RA-5.
CM-8	Operational	Configuration Management	Information System Component Inventory	P1	The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes [Assignment: organization-defined information deemed necessary to achieve effective property accountability]; and e. Is available for review and audit by designated organizational officials.	Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address. Related controls: CM-2, CM-6.
CM-9	Operational	Configuration Management	Configuration Management Plan	P1	The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration managed. The configuration management plan satisfies the requirements in the organization's configuration management policy while being tailored to the individual information system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. The plan describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated. The configuration management approval process includes designation of key management stakeholders that are responsible for reviewing and approving proposed changes to the information system, and security personnel that would conduct an impact analysis prior to the implementation of any changes to the system. Related control: SA-10.
CP-1	Operational	Contingency Planning	Contingency Planning Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the contingency planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the contingency planning policy. Related control: PM-9.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
CP-2	Operational	Contingency Planning	Contingency Plan	P1	The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements].	Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Information system recovery objectives are consistent with applicable laws, Executive Orders, directives, policies, standards, or regulations. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack. Related controls: AC-14, CP-6, CP-7, CP-8, IR-4, PM-8, PM-11.
CP-3	Operational	Contingency Planning	Contingency Training	P2	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency].	None.
CP-4	Operational	Contingency Planning	Contingency Plan Testing and Exercises	P2	The organization: a. Tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Reviews the contingency plan test/exercise results and initiates corrective actions.	There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation: parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan.
CP-6	Operational	Contingency Planning	Alternate Storage Site	P1	The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.	Related controls: CP-2, CP-9, MP-4.

Ref	Class	Type	Name	Priority	Description	Guidance
CP-7	Operational	Contingency Planning	Alternate Processing Site	P1	The organization: a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period consistent with recovery time objectives] when the primary processing capabilities are unavailable; and b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.	Related control: CP-2.
CP-8	Operational	Contingency Planning	Telecommunications Services	P1	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.	Related control: CP-2.
CP-9	Operational	Contingency Planning	Information System Backup	P1	The organization: a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protects the confidentiality and integrity of backup information at the storage location.	System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organizational assessment of risk guides the use of encryption for protecting backup information. The protection of system backup information while in transit is beyond the scope of this control. Related controls: CP-6, MP-4.
CP-10	Operational	Contingency Planning	Information System Recovery and Reconstitution	P1	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	Recovery is executing information system contingency plan activities to restore essential missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation. Recovery and reconstitution procedures are based on organizational priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure. Recovery and reconstitution capabilities employed by the organization can be a combination of automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, SC-24.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
IR-1	Operational	Incident Response	Incident Response Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the incident response family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the incident response policy. Related control: PM-9.
IR-2	Operational	Incident Response	Incident Response Training	P2	The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and b. Provides refresher training [Assignment: organization-defined frequency].	Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related control: AT-3.
IR-3	Operational	Incident Response	Incident Response Testing and Exercises	P2	The organization tests and/or exercises the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.	None.
IR-4	Operational	Incident Response	Incident Handling	P1	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, CP-2, IR-2, IR-3, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.
IR-5	Operational	Incident Response	Incident Monitoring	P1	The organization tracks and documents information system security incidents.	Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Ref	Class	Type	Name	Priority	Description	Guidance
IR-6	Operational	Incident Response	Incident Reporting	P1	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time-period]; and b. Reports security incident information to designated authorities.	The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5.
IR-7	Operational	Incident Response	Incident Response Assistance	P3	The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. Related controls: IR-4, IR-6.
IR-8	Operational	Incident Response	Incident Response Plan	P1	The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements].	It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization's mission, strategies, and goals for incident response help determine the structure of its incident response capability.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
MA-1	Operational	Maintenance	System Maintenance Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system maintenance family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system maintenance policy. Related control: PM-9.
MA-2	Operational	Maintenance	Controlled Maintenance	P2	The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	The control is intended to address the information security aspects of the organization's information system maintenance program. Related controls: MP-6, SI-2.
MA-3	Operational	Maintenance	Maintenance Tools	P2	The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.	The intent of this control is to address the security-related issues arising from the hardware and software brought into the information system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control. Related control: MP-6.

Ref	Class	Type	Name	Priority	Description	Guidance
MA-4	Operational	Maintenance	Non-Local Maintenance	P1	The organization: a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed.	Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Identification and authentication techniques used in the establishment of non-local maintenance and diagnostic sessions are consistent with the network access requirements in IA-2. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part, by other controls. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-8, MA-5, MP-6, SC-7.
MA-5	Operational	Maintenance	Maintenance Personnel	P1	The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for a very limited time period. Related controls: IA-8, MA-5.
MA-6	Operational	Maintenance	Timely Maintenance	P1	The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined list of security-critical information system components and/or key IT components] within [Assignment: organization-defined time period] of failure.	The organization specifies those information system components that, when not operational, result in increased risk to organizations, individuals, or the Nation because the security functionality intended by that component is not being provided. Security-critical components include, for example, firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems. Related control: CP-2.
MP-1	Operational	Media Protection	Media Protection Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the media protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the media protection policy. Related control: PM-9.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
MP-2	Operational	Media Protection	Media Access	P1	The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals] using [Assignment: organization-defined security measures].	Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection. Related controls: MP-4, PE-3.
MP-3	Operational	Media Protection	Media Marking	P1	The organization: a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [Assignment: organization-defined list of removable media types] from marking as long as the exempted items remain within [Assignment: organization-defined controlled areas].	The term marking is used when referring to the application or use of human-readable security attributes. The term labeling is used when referring to the application or use of security attributes with regard to internal data structures within the information system (see AC-16, Security Attributes). Removable information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). An organizational assessment of risk guides the selection of media requiring marking. Marking is generally not required for media containing information determined by the organization to be in the public domain or to be publicly releasable. Some organizations, however, may require markings for public information indicating that the information is publicly releasable. Organizations may extend the scope of this control to include information system output devices containing organizational information, including, for example, monitors and printers. Marking of removable media and information system output is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
MP-4	Operational	Media Protection	Media Storage	P1	The organization: a. Physically controls and securely stores [Assignment: organization-defined types of digital and non-digital media] within [Assignment: organization-defined controlled areas] using [Assignment: organization-defined security measures]; b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Telephone systems are

Ref	Class	Type	Name	Priority	Description	Guidance
						also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use extreme caution in the types of information stored on telephone voicemail systems. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections are sufficient to meet the requirements established for protecting the information and/or information system. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. As part of a defense-in-depth strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. The employment of cryptography is at the discretion of the information owner/steward. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information. The strength of mechanisms is commensurate with the classification and sensitivity of the information. Related controls: AC-3, AC-19, CP-6, CP-9, MP-2, PE-3.
MP-5	Operational	Media Protection	Media Transport	P1	The organization: a. Protects and controls [Assignment: organization-defined types of digital and non-digital media] during transport outside of controlled areas using [Assignment: organization-defined security measures]; b. Maintains accountability for information system media during transport outside of controlled areas; and c. Restricts the activities associated with transport of such media to authorized personnel.	Information system media includes both digital media (e.g., diskettes, magnetic tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
						Physical and technical security measures for the protection of digital and non-digital media are commensurate with the classification or sensitivity of the information residing on the media, and consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Locked containers and cryptography are examples of security measures available to protect digital and non-digital media during transport. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used. An organizational assessment of risk guides: (i) the selection of media and associated information contained on that media requiring protection during transport; and (ii) the selection and use of storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Related controls: AC-19, CP-9.
MP-6	Operational	Media Protection	Media Sanitization	P1	The organization: a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.	This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or released for disposal. The organization uses its discretion on the employment of sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposal.
PS-1	Operational	Personnel Security	Personnel Security Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the personnel security family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the personnel security policy. Related control: PM-9.
PS-2	Operational	Personnel Security	Position Categorization	P1	The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations [Assignment: organization-defined frequency].	Position risk designations are consistent with Office of Personnel Management policy and guidance. The screening criteria include explicit information security role appointment requirements (e.g., training, security clearance).

Ref	Class	Type	Name	Priority	Description	Guidance
PS-3	Operational	Personnel Security	Personnel Screening	P1	The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening].	Screening and rescreening are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position. The organization may define different rescreening conditions and frequencies for personnel accessing the information system based on the type of information processed, stored, or transmitted by the system.
PS-4	Operational	Personnel Security	Personnel Termination	P2	The organization, upon termination of individual employment: a. Terminates information system access; b. Conducts exit interviews; c. Retrieves all security-related organizational information system-related property; and d. Retains access to organizational information and information systems formerly controlled by terminated individual.	Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that individuals understand any security constraints imposed by being former employees and that proper accountability is achieved for all information system-related property. Exit interviews may not be possible for some employees (e.g., in the case of job abandonment, some illnesses, and nonavailability of supervisors). Exit interviews are important for individuals with security clearances. Timely execution of this control is particularly essential for employees or contractors terminated for cause.
PS-5	Operational	Personnel Security	Personnel Transfer	P2	The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action].	This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted. In addition the organization defines the actions appropriate for the type of reassignment or transfer; whether permanent or temporary. Actions that may be required when personnel are transferred or reassigned to other positions within the organization include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing previous information system accounts and establishing new accounts; (iii) changing information system access authorizations; and (iv) providing for access to official records to which the employee had access at the previous work location and in the previous information system accounts.
PS-6	Operational	Personnel Security	Access Agreements	P3	The organization: a. Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements [Assignment: organization-defined frequency].	Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy. Related control: PL-4.
PS-7	Operational	Personnel Security	Third-Party Personnel Security	P1	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance.	Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, IT services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents.
PS-8	Operational	Personnel Security	Personnel Sanctions	P3	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	The sanctions process is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The process is described in access agreements and can be included as part of the general personnel policies and procedures for the organization. Related controls: PL-4, PS-6.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
PE-1	Operational	Physical & Environmental Protection	Physical and Environmental Protection Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the physical and environmental protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the physical and environmental protection policy. Related control: PM-9.
PE-2	Operational	Physical & Environmental Protection	Physical Access Authorizations	P1	The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials [Assignment: organization-defined frequency], removing from the access list personnel no longer requiring access.	Authorization credentials include, for example, badges, identification cards, and smart cards. Related controls: PE-3, PE-4.
PE-3	Operational	Physical & Environmental Protection	Physical Access Control	P1	The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices [Assignment: organization-defined frequency]; and g. Changes combinations and keys [Assignment: organization-defined frequency] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.	The organization determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being safeguarded. Related controls: MP-2, MP-4, PE-2.

Ref	Class	Type	Name	Priority	Description	Guidance
PE-4	Operational	Physical & Environmental Protection	Access Control for Transmission Medium	P1	The organization controls physical access to information system distribution and transmission lines within organizational facilities.	Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related control: PE-2.
PE-5	Operational	Physical & Environmental Protection	Access Control for Output Devices	P1	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	Monitors, printers, and audio devices are examples of information system output devices.
PE-6	Operational	Physical & Environmental Protection	Monitoring Physical Access	P1	The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs [Assignment: organization-defined frequency]; and c. Coordinates results of reviews and investigations with the organization's incident response capability.	Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability.
PE-7	Operational	Physical & Environmental Protection	Visitor Control	P1	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.	Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.
PE-8	Operational	Physical & Environmental Protection	Access Records	P3	The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and b. Reviews visitor access records [Assignment: organization-defined frequency].	Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited.
PE-9	Operational	Physical & Environmental Protection	Power Equipment and Power Cabling	P1	The organization protects power equipment and power cabling for the information system from damage and destruction.	This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.
PE-10	Operational	Physical & Environmental Protection	Emergency Shutoff	P1	The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	This control applies to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.
PE-11	Operational	Physical & Environmental Protection	Emergency Power	P1	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
PE-12	Operational	Physical & Environmental Protection	Emergency Lighting	P1	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.
PE-13	Operational	Physical & Environmental Protection	Fire Protection	P1	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.
PE-14	Operational	Physical & Environmental Protection	Temperature and Humidity Controls	P1	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and b. Monitors temperature and humidity levels [Assignment: organization-defined frequency].	This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.
PE-15	Operational	Physical & Environmental Protection	Water Damage Protection	P1	The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.
PE-16	Operational	Physical & Environmental Protection	Delivery and Removal	P1	The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.	Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.
PE-17	Operational	Physical & Environmental Protection	Alternate Work Site	P1	The organization: a. Employs [Assignment: organization-defined management, operational, and technical information system security controls] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	Alternate work sites may include, for example, government facilities or private residences of employees. The organization may define different sets of security controls for specific alternate work sites or types of sites.
PE-18	Operational	Physical & Environmental Protection	Location of Information System Components	P2	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards. In addition, the organization considers the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to the information system and therefore, increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Ref	Class	Type	Name	Priority	Description	Guidance
PE-19	Operational	Physical & Environmental Protection	Information Leakage	P0	The organization protects the information system from information leakage due to electromagnetic signals emanations.	The security categorization of the information system (with respect to confidentiality) and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.
SI-1	Operational	System & Information Integrity	System and Information Integrity Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and information integrity family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and information integrity policy. Related control: PM-9.
SI-2	Operational	System & Information Integrity	Flaw Remediation	P1	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process.	The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in US-CERT guidance and Information Assurance Vulnerability Alerts have been accomplished. Related controls: CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
SI-3	Operational	System & Information Integrity	Malicious Code Protection	P1	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: - Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and - [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyberattacks that could affect organizational missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended. Related controls: SA-4, SA-8, SA-12, SA-13, SI-4, SI-7.
SI-4	Operational	System & Information Integrity	Information System Monitoring	P1	The organization: a. Monitors events on the information system in accordance with [Assignment: organization-defined monitoring objectives] and detects information system attacks; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.	Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. The Einstein network monitoring device from the Department of Homeland Security is an example of a system monitoring device. The granularity of the information collected is determined by the organization based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP proxies, when use of such proxies is required. Related controls: AC-4, AC-8, AC-17, AU-2, AU-6, SI-3, SI-7.

Ref	Class	Type	Name	Priority	Description	Guidance
SI-5	Operational	System & Information Integrity	Security Alerts, Advisories, and Directives	P1	The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to [Assignment: organization-defined list of personnel (identified by name and/or by role)]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	Security alerts and advisories are generated by the United States Computer Emergency Readiness Team (US-CERT) to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.
SI-6	Operational	System & Information Integrity	Security Functionality Verification	P1	The information system verifies the correct operation of security functions [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator; shuts the system down; restarts the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.	The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required. Information system transitional states include, for example, startup, restart, shutdown, and abort.
SI-7	Operational	System & Information Integrity	Software and Information Integrity	P1	The information system detects unauthorized changes to software and information.	The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.
SI-8	Operational	System & Information Integrity	Spam Protection	P1	The organization: a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.	Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Related controls: SC-5, SI-3.
SI-9	Operational	System & Information Integrity	Information Input Restrictions	P2	The organization restricts the capability to input information to the information system to authorized personnel.	Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. Related controls: AC-5, AC-6.
SI-10	Operational	System & Information Integrity	Information Input Validation	P1	The information system checks the validity of information inputs.	Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
SI-11	Operational	System & Information Integrity	Error Handling	P2	The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing [Assignment: organization-defined sensitive or potentially harmful information] in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel.	The structure and content of error messages are carefully considered by the organization. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Sensitive information includes, for example, account numbers, social security numbers, and credit card numbers.
SI-12	Operational	System & Information Integrity	Information Output Handling and Retention	P2	The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The output handling and retention requirements cover the full life cycle of the information, in some cases extending beyond the disposal of the information system. The National Archives and Records Administration provides guidance on records retention. Related controls: MP-2, MP-4.
SI-13	Operational	System & Information Integrity	Predictable Failure Prevention	P0	The organization: a. Protects the information system from harm by considering mean time to failure for [Assignment: organization-defined list of information system components] in specific environments of operation; and b. Provides substitute information system components, when needed, and a mechanism to exchange active and standby roles of the components.	While mean time to failure is primarily a reliability issue, this control focuses on the potential failure of specific components of the information system that provide security capability. Mean time to failure rates are defendable and based on considerations that are installation-specific, not industry-average. The transfer of responsibilities between active and standby information system components does not compromise safety, operational readiness, or security (e.g., state variables are preserved). The standby component is available at all times except where a failure recovery is in progress or for maintenance reasons. Related control: CP-2.
AC-1	Technical	Access Control	Access Control Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy. Related control: PM-9.
AC-2	Technical	Access Control	Account Management	P1	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts; f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;	The identification of authorized users of the information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-4, IA-5, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.

Ref	Class	Type	Name	Priority	Description	Guidance
					g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and j. Creating a process for reviewing and notifying accounts' status [Assignment: organization-defined frequency].	
AC-3	Technical	Access Control	Access Enforcement	P1	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information-system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. For classified information, the cryptography used is largely dependent on the classification level of the information and the clearances of the individuals having access to the information. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.
AC-4	Technical	Access Control	Information Flow Enforcement	P1	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few examples of flow control restrictions include: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
						and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content (e.g., using key word searches or document characteristics). Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls. Related controls: AC-17, AC-19, AC-21, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.
AC-5	Technical	Access Control	Separation of Duties	P1	The organization: a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion; b. Documents separation of duties; and c. Implements separation of duties through assigned information system access authorizations.	Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles. Access authorizations defined in this control are implemented by control AC-3. Related control: AC-3.
AC-6	Technical	Access Control	Least Privilege	P1	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Related controls: AC-2, AC-3, CM-7.
AC-7	Technical	Access Control	Unsuccessful Login Attempts	P2	The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid login attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next login prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may choose to employ different algorithms for different information system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels. This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14.
AC-8	Technical	Access Control	System Use Notification	P1	The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy, LEGAL and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of	System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an interactive interface does not exist.

Ref	Class	Type	Name	Priority	Description	Guidance
					the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.	
AC-9	Technical	Access Control	Previous Logon (Access) Notification	P0	The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).	This control is intended to cover both traditional logons to information systems and general accesses to information systems that occur in other types of architectural configurations (e.g., service oriented architectures).
AC-10	Technical	Access Control	Concurrent Session Control	P2	The information system limits the number of concurrent sessions for each system account to [Assignment: organization-defined number].	The organization may define the maximum number of concurrent sessions for an information system account globally, by account type, by account, or a combination. This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts.
AC-11	Technical	Access Control	Session Lock	P3	The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.
AC-14	Technical	Access Control	Permitted Actions Without Identification Or Authentication	P1	The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.	This control is intended for those specific instances where an organization determines that no identification and authentication is required; it is not, however, mandating that such instances exist in given information system. The organization may allow a limited number of user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible federal information systems such as http://www.usa.gov). Organizations also identify any actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypass may be, for example, via a software-readable physical switch that commands bypass of the login functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not being repeated, but rather to situations where identification and/or authentication have not yet occurred. Related controls: CP-2, IA-2.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
AC-16	Technical	Access Control	Security Attributes	P0	The information system supports and maintains the binding of [Assignment: organization-defined security attributes] to information in storage, in process, and in transmission.	Security attributes are abstractions representing the basic properties or characteristics of an entity (e.g., subjects and objects) with respect to safeguarding information. These attributes are typically associated with internal data structures (e.g., records, buffers, files) within the information system and are used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy. The term security label is often used to associate a set of security attributes with a specific information object as part of the data structure for that object (e.g., user access privileges, nationality, affiliation as contractor). Related controls: AC-3, AC-4, SC-16, MP-3.
AC-17	Technical	Access Control	Remote Access	P1	The organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system.	This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3. Related controls: AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4.
AC-18	Technical	Access Control	Wireless Access	P1	The organization: a. Establishes usage restrictions and implementation guidance for wireless access; b. Monitors for unauthorized wireless access to the information system; c. Authorizes wireless access to the information system prior to connection; and d. Enforces requirements for wireless connections to the information system.	Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of organization-controlled facilities. Related controls: AC-3, IA-2, IA-3, IA-8.

Ref	Class	Type	Name	Priority	Description	Guidance
AC-19	Technical	Access Control	Access Control for Mobile Devices	P1	The organization: a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; c. Monitors for unauthorized connections of mobile devices to organizational information systems; d. Enforces requirements for the connection of mobile devices to organizational information systems; e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and g. Applies [Assignment: organization-defined inspection and preventative measures] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.	Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security requirements. Usage restrictions and implementation guidance related to mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay. Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family. Related controls: MP-4, MP-5.
AC-20	Technical	Access Control	Use of External Information Systems	P1	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, and/or transmit organization-controlled information using the external information systems.	External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
						are not owned by, operated by, or under the direct supervision and authority of the organization. For some external systems, in particular those systems operated by other federal agencies, including organizations subordinate to those agencies, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or organizations subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system and over which the organization has the authority to impose rules of behavior with regard to system access. The restrictions that an organization imposes on authorized individuals need not be uniform, as those restrictions are likely to vary depending upon the trust relationships between organizations. Thus, an organization might impose more stringent security restrictions on a contractor than on a state, local, or tribal government. This control does not apply to the use of external information systems to access public interfaces to organizational information systems and information (e.g., individuals accessing federal information through www.usa.gov). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system. This control defines access authorizations enforced by AC-3, rules of behavior requirements enforced by PL-4, and session establishment rules enforced by AC-17. Related controls: AC-3, AC-17, PL-4.
AC-21	Technical	Access Control	User-Based Collaboration and Information Sharing	P0	The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employs [Assignment: list of organization-defined information sharing circumstances and automated mechanisms or manual processes required] to assist users in making information sharing/collaboration decisions.	The control applies to information that may be restricted in some manner (e.g., privileged medical, contract-sensitive, proprietary, PII, special access programs/compartments) based on some formal or administrative determination. Depending on the information-sharing circumstance, the sharing partner may be defined at the individual, group, or organization level and information may be defined by specific content, type, or security categorization. Related control: AC-3.

Ref	Class	Type	Name	Priority	Description	Guidance
AC-22	Technical	Access Control	Publicly Accessible Content	P2	The organization: a. Designates individuals authorized to post information onto an organizational information system that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information [Assignment: organization-defined frequency]; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.	Nonpublic information is any information for which the general public is not authorized access in accordance with federal laws, Executive Orders, directives, policies, regulations, standards, or guidance. Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This control addresses posting information on an organizational information system that is accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by appropriate organizational policy. Related controls: AC-3, AU-13.
AU-1	Technical	Audit & Accountability	Audit and Accountability Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the audit and accountability family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the audit and accountability policy. Related control: PM-9.
AU-2	Technical	Audit & Accountability	Auditable Events	P1	The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [Assignment: organization-defined list of auditable events]; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event].	The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are to be audited at a given point in time. For example, the organization may determine that the information system must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Related control: AU-3.
AU-3	Technical	Audit & Accountability	Content of Audit Records	P1	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Related controls: AU-2, AU-8.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
AU-4	Technical	Audit & Accountability	Audit Storage Capacity	P1	The organization allocates audit record storage capacity and configures auditing IN CONSULTATION WITH LEGAL TEAMS to reduce the likelihood of such capacity being exceeded.	The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Related controls: AU-2, AU-5, AU-6, AU-7, SI-4.
AU-5	Technical	Audit & Accountability	Response To Audit Processing Failures	P1	The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.
AU-6	Technical	Audit & Accountability	Audit Review, Analysis, and Reporting	P1	The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	Related control: AU-7.
AU-7	Technical	Audit & Accountability	Audit Reduction and Report Generation	P2	The information system provides an audit reduction and report generation capability.	An audit reduction and report generation capability provides support for near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records. Related control: AU-6.
AU-8	Technical	Audit & Accountability	Time Stamps	P1	The information system uses internal system clocks to generate time stamps for audit records.	Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Related control: AU-3.
AU-9	Technical	Audit & Accountability	Protection of Audit Information	P1	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. Related controls: AC-3, AC-6.
AU-10	Technical	Audit & Accountability	Non-Repudiation	P1	The information system protects against an individual falsely denying having performed a particular action.	Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

Ref	Class	Type	Name	Priority	Description	Guidance
AU-11	Technical	Audit & Accountability	Audit Record Retention	P3	The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. The National Archives and Records Administration (NARA) General Records Schedules (GRS) provide federal policy on record retention.
AU-12	Technical	Audit & Accountability	Audit Generation	P1	The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [Assignment: organization-defined information system components]; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	Audits records can be generated from various components within the information system. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events). Related controls: AU-2, AU-3.
AU-13	Technical	Audit & Accountability	Monitoring for Information Disclosure	P0	The organization monitors open source information for evidence of unauthorized exfiltration or disclosure of organizational information [Assignment: organization-defined frequency].	None.
AU-14	Technical	Audit & Accountability	Session Audit	P0	The information system provides the capability to: a. Capture/record and log all content related to a user session; and b. Remotely view/hear all content related to an established user session in real time.	Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
IA-1	Technical	Identification & Authentication	Identification and Authentication Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. c. POLICY HAS TO BE SIGNED BY THE INFORMATION SECURITY OFFICER AND SIGNED BY ALL EMPLOYEES.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the identification and authentication family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the identification and authentication policy. Related control: PM-9.
IA-2	Technical	Identification & Authentication	Identification and Authentication (Organizational Users)	P1	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
						accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Access to organizational information systems is defined as either local or network. Local access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization. For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than organizational users are described in IA-8. The identification and authentication requirements in this control are satisfied by complying with Homeland Security Presidential Directive 12 consistent with organization-specific implementation plans provided to OMB. In addition to identifying and authenticating users at the information-system level (i.e., at logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Related controls: AC-14, AC-17, AC-18, IA-4, IA-5.
IA-3	Technical	Identification & Authentication	Device Identification and Authentication	P1	The information system uniquely identifies and authenticates [Assignment: organization-defined list of specific and/or types of devices] before establishing a connection.	The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for identification or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the security categorization of the information system.

Ref	Class	Type	Name	Priority	Description	Guidance
IA-4	Technical	Identification & Authentication	Identifier Management	P1	The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers for [Assignment: organization-defined time period]; and e. Disabling the user identifier after [Assignment: organization-defined time period of inactivity].	Common device identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device-unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the account management activities of AC-2. IA-4 also covers user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system). Related controls: AC-2, IA-2.
IA-5	Technical	Identification & Authentication	Authenticator Management	P1	The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.	User authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The requirement to protect user authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of users and by controls AC-3, AC-6, and SC-28 for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The information system supports user authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one time tokens, and number of allowed rejections during verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, IA-2, PL-4, PS-6.
IA-6	Technical	Identification & Authentication	Authenticator Feedback	P1	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.
IA-7	Technical	Identification & Authentication	Cryptographic Module Authentication	P1	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	None.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
IA-8	Technical	Identification & Authentication	Identification and Authentication (Non-Organizational Users)	P1	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	Non-organizational users include all information system users other than organizational users explicitly covered by IA-2. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Accordingly, a risk assessment is used in determining the authentication needs of the organization. Scalability, practicality, and security are simultaneously considered in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. Identification and authentication requirements for information system access by organizational users are described in IA-2. Related controls: AC-14, AC-17, AC-18, MA-4.
SC-1	Technical	System & Communications Protection	System and Communications Protection Policy and Procedures	P1	The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and communications protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and communications protection policy. Related control: PM-9.
SC-2	Technical	System & Communications Protection	Application Partitioning	P1	The information system separates user functionality (including user interface services) from information system management functionality.	Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.

Ref	Class	Type	Name	Priority	Description	Guidance
SC-3	Technical	System & Communications Protection	Security Function Isolation	P1	The information system isolates security functions from non-security functions.	The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process. Related control: SA-13.
SC-4	Technical	System & Communications Protection	Information In Shared Resources	P1	The information system prevents unauthorized and unintended information transfer via shared system resources.	The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.
SC-5	Technical	System & Communications Protection	Denial of Service Protection	P1	The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].	A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks. Related control: SC-7.
SC-6	Technical	System & Communications Protection	Resource Priority	P0	The information system limits the use of resources by priority.	Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process. This control does not apply to components in the information system for which there is only a single user/role.
SC-7	Technical	System & Communications Protection	Boundary Protection	P1	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
						attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-4, IR-4, SC-5.
SC-8	Technical	System & Communications Protection	Transmission Integrity	P1	The information system protects the integrity of transmitted information.	This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.
SC-9	Technical	System & Communications Protection	Transmission Confidentiality	P1	The information system protects the confidentiality of transmitted information.	This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.
SC-10	Technical	System & Communications Protection	Network Disconnect	P2	The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. The time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses.
SC-11	Technical	System & Communications Protection	Trusted Path	P0	The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication].	A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).
SC-12	Technical	System & Communications Protection	Cryptographic Key Establishment and Management	P1	The organization establishes and manages cryptographic keys for required cryptography employed within the information system.	Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

Ref	Class	Type	Name	Priority	Description	Guidance
SC-13	Technical	System & Communications Protection	Use of Cryptography	P1	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	None.
SC-14	Technical	System & Communications Protection	Public Access Protections	P1	The information system protects the integrity and availability of publicly available information and applications.	The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.
SC-15	Technical	System & Communications Protection	Collaborative Computing Devices	P1	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and b. Provides an explicit indication of use to users physically present at the devices.	Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.
SC-16	Technical	System & Communications Protection	Transmission of Security Attributes	P0	The information system associates security attributes with information exchanged between information systems.	Security attributes may be explicitly or implicitly associated with the information contained within the information system. Related control: AC-16.
SC-17	Technical	System & Communications Protection	Public Key Infrastructure Certificates	P1	The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates under an appropriate certificate policy from an approved service provider.	For user certificates, each organization attains certificates from an approved, shared service provider, as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified with the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice. This control focuses on certificates with a visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services.
SC-18	Technical	System & Communications Protection	Mobile Code	P1	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.	Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Policy and procedures related to mobile code, address preventing the development, acquisition, or introduction of unacceptable mobile code within the information system.
SC-19	Technical	System & Communications Protection	Voice Over Internet Protocol	P1	The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.	None.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
SC-20	Technical	System & Communications Protection	Secure Name / Address Resolution Service (Authoritative Source)	P1	The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.	This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23.
SC-21	Technical	System & Communications Protection	Secure Name / Address Resolution Service (Recursive Or Caching Resolver)	P1	The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.	A recursive resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients. Authoritative DNS servers are examples of authoritative sources. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.
SC-22	Technical	System & Communications Protection	Architecture and Provisioning for Name / Address Resolution Service	P1	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). With regard to role separation, DNS servers with an internal role, only process name/address resolution requests from within the organization (i.e., internal clients). DNS servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the external networks including the Internet). The set of clients that can access an authoritative DNS server in a particular role is specified by the organization (e.g., by address ranges, explicit lists).
SC-23	Technical	System & Communications Protection	Session Authenticity	P1	The information system provides mechanisms to protect the authenticity of communications sessions.	This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).

Ref	Class	Type	Name	Priority	Description	Guidance
SC-24	Technical	System & Communications Protection	Fail In Known State	P1	The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.	Failure in a known state can address safety or security in accordance with the mission/business needs of the organization. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of the organization with less disruption of mission/business processes.
SC-25	Technical	System & Communications Protection	Thin Nodes	P0	The information system employs processing components that have minimal functionality and information storage.	The deployment of information system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to a successful attack. Related control: SC-30.
SC-26	Technical	System & Communications Protection	Honeypots	P0	The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.	None.
SC-27	Technical	System & Communications Protection	Operating System-Independent Applications	P0	The information system includes: [Assignment: organization-defined operating system-independent applications].	Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, increasing the availability for critical functionality within an organization while information systems with a given operating system are under attack.
SC-28	Technical	System & Communications Protection	Protection of Information At Rest	P1	The information system protects the confidentiality and integrity of information at rest.	This control is intended to address the confidentiality and integrity of information at rest in nonmobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system. Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information likely requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.
SC-29	Technical	System & Communications Protection	Heterogeneity	P0	The organization employs diverse information technologies in the implementation of the information system.	Increasing the diversity of information technologies within the information system reduces the impact of the exploitation of a specific technology. Organizations that select this control should consider that an increase in diversity may add complexity and management overhead, both of which have the potential to lead to mistakes and misconfigurations which could increase overall risk.
SC-30	Technical	System & Communications Protection	Virtualization Techniques	P0	The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations.	Virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.

(continued on next page)

Ref	Class	Type	Name	Priority	Description	Guidance
SC-31	Technical	System & Communications Protection	Covert Channel Analysis	P0	The organization requires that information system developers/integrators perform a covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels.	Information system developers/integrators are in the best position to identify potential avenues within the system that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, for example, in the case of information systems containing export-controlled information and having connections to external networks (i.e., networks not controlled by the organization). Covert channel analysis is also meaningful in the case of multilevel secure (MLS) systems, multiple security level (MSL) systems, and cross domain systems.
SC-32	Technical	System & Communications Protection	Information System Partitioning	P1	The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.	Information system partitioning is a part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components. Related controls: AC-4, SC-7.
SC-33	Technical	System & Communications Protection	Transmission Preparation Integrity	P0	The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.	Information can be subjected to unauthorized changes (e.g., malicious and/or unintentional modification) at information aggregation or protocol transformation points.
SC-34	Technical	System & Communications Protection	Non-Modifiable Executable Programs	P0	The information system at [Assignment: organization-defined information system components]: a. Loads and executes the operating environment from hardware-enforced, read-only media; and b. Loads and executes [Assignment: organization-defined applications] from hardware-enforced, read-only media.	In this control, the term operating environment is defined as the code upon which applications are hosted, for example, a monitor, executive, operating system, or application running directly on the hardware platform. Hardware-enforced, read-only media include, for example, CD-R/DVD-R disk drives. Use of non-modifiable storage ensures the integrity of the software program from the point of creation of the read-only image.

Source: NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.

APPENDIX D

Using the Multimedia Material

Instructions

Multimedia material including narrated training lessons, a training poster, and a library of references can be found on the accompanying CD-ROM. The objective of this material is to provide airport staff with instruction on the primary cybersecurity best practices expected of them. The multimedia material also offers senior managers, IT professionals, and consultants instruction and helpful resources with regard to cybersecurity.

Once placed into a CD/DVD drive on a computer, the CD should start; navigate to the CD menu and click on Multimedia Material. If the CD does not start automatically, open up a file browser, navigate to and click on START.html in the root directory.

The multimedia material is primarily designed to be viewed by airport staff, senior managers, IT personnel, and consultants/tenants. When it first opens, a brief lesson will play that explains these roles and how to get started using the material. The four characters that are used throughout the material to represent these four primary roles are introduced in this first lesson. When this lesson concludes, the Role toolbox should slide out and the screen should look like Figure 7.

Figure 7. Multimedia main screen.

Figure 8. Multimedia toolboxes.

To get started, click on the role in the Role toolbox that best matches your position. Other toolboxes will appear with content that is customized for your role as shown in Figure 8. The lessons are narrated, so please make sure sound is on. All spoken words appear as text as well.

Buttons appear in the top banner of all of the toolboxes. Clicking on the question mark will bring up the help file. Clicking on the red arrow will collapse the toolbox to display just the banner to free up screen space. Clicking on the red "X" will close the toolbox, causing it to shrink to an icon that is docked on the left side of the screen. Clicking on this icon will reopen the toolbox.

The Content toolbox displays a hierarchical outline of the topics available. Click on the "+" and "–" signs to expand and collapse sub-topics, respectively. Once you click on a topic, the lesson will start in the right-hand portion of the screen. When a lesson is complete, select another topic. Although the lessons are arranged in an order, you can view them in any order you wish.

The Library toolbox functions in a similar way to the Content toolbox but displays references and resources that may be of interest to you. Although each lesson is timed to run at a particular pace, you can use the controls at the lower right-hand side of the screen (Figure 9) to play, pause, advance, or rewind the presentation.

Figure 9. Presentation controls.

The Search tool allows you to enter keywords as search criteria. Over 60 documents identified as being relevant to airport cybersecurity during the literature search portion of this project will be searched. This tool doesn't slide out by default when the application opens but, like other tools, can be opened by clicking on its icon on the left-hand side of the screen. After entering keyword(s)

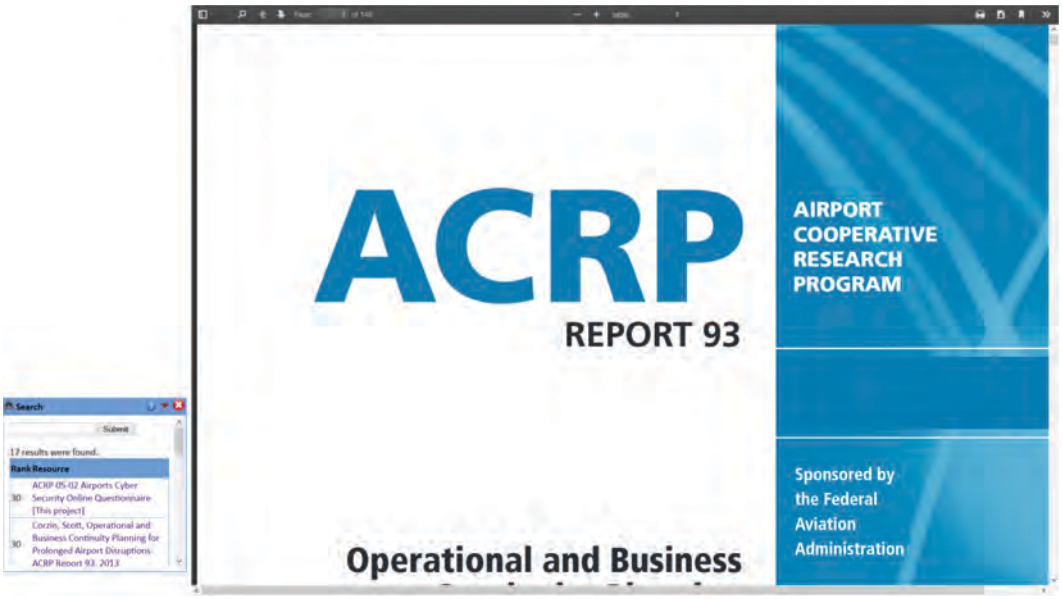


Figure 10. Multimedia document search.

into the search criteria textbox, click Submit to list documents that contain the words entered. This list is ranked in descending order of relevance, as determined by a count of keywords associated with each document. Clicking on the link associated with each search result will bring up the document in the primary right-hand panel, as shown in Figure 10. At the bottom of the list is a link to clear the results so that another search can be performed. The list can also be cleared by simply typing in new keyword(s) and clicking Submit.

Technical Considerations

The multimedia material operates within a standard web browser (Internet Explorer and Firefox were tested). If the material does not open, try a different web browser. All functionality is delivered using HTML5, CSS, and JavaScript technology. JQuery is used for some functions. No proprietary software is required. All content with the exception of most of the documents referenced in the library are links to locations on the Internet. These links were current upon publication of this document.

The configuration of the roles and content is handled by XML files in the root directory of the application. Individuals familiar with editing XML can adjust or add to this content as they wish. The actual lessons cannot be changed, but they can be added or removed if desired.

Abbreviations and acronyms used without definitions in TRB publications:

A4A	Airlines for America
AAAE	American Association of Airport Executives
AASHO	American Association of State Highway Officials
AASHTO	American Association of State Highway and Transportation Officials
ACI–NA	Airports Council International–North America
ACRP	Airport Cooperative Research Program
ADA	Americans with Disabilities Act
APTA	American Public Transportation Association
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
ATA	American Trucking Associations
CTAA	Community Transportation Association of America
CTBSSP	Commercial Truck and Bus Safety Synthesis Program
DHS	Department of Homeland Security
DOE	Department of Energy
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FMCSA	Federal Motor Carrier Safety Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
HMCRP	Hazardous Materials Cooperative Research Program
IEEE	Institute of Electrical and Electronics Engineers
ISTEA	Intermodal Surface Transportation Efficiency Act of 1991
ITE	Institute of Transportation Engineers
MAP-21	Moving Ahead for Progress in the 21st Century Act (2012)
NASA	National Aeronautics and Space Administration
NASAO	National Association of State Aviation Officials
NCFRP	National Cooperative Freight Research Program
NCHRP	National Cooperative Highway Research Program
NHTSA	National Highway Traffic Safety Administration
NTSB	National Transportation Safety Board
PHMSA	Pipeline and Hazardous Materials Safety Administration
RITA	Research and Innovative Technology Administration
SAE	Society of Automotive Engineers
SAFETEA-LU	Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (2005)
TCRP	Transit Cooperative Research Program
TEA-21	Transportation Equity Act for the 21st Century (1998)
TRB	Transportation Research Board
TSA	Transportation Security Administration
U.S.DOT	United States Department of Transportation

THE NATIONAL ACADEMIES™

Advisers to the Nation on Science, Engineering, and Medicine

The nation turns to the National Academies—National Academy of Sciences, National Academy of Engineering, Institute of Medicine, and National Research Council—for independent, objective advice on issues that affect people's lives worldwide.

www.national-academies.org

ISBN 978-0-309-30880-9

90000

9 780309 308809

TRANSPORTATION RESEARCH BOARD
500 Fifth Street, NW
Washington, DC 20001

ADDRESS SERVICE REQUESTED

NON-PROFIT ORG.
U.S. POSTAGE
PAID
COLUMBIA, MD
PERMIT NO. 88