NIST Special Publication 800-12 (DRAFT)
Revision 1

An Introduction to Information Security

Michael Nieles
Kelley Dempsey
Victoria Yan Pillitteri

COMPUTER SECURITY

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-12 (DRAFT)
Revision 1

An Introduction to Information Security

Michael Nieles
Kelley Dempsey
Victoria Yan Pillitteri
Computer Security Division
Information Technology Laboratory

January 2017

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-12 Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-12 Rev. 1, 97 pages (January 2017)
CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: *January 23, 2017* through *February 22, 2017*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: SP800-12-DRAFT@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in systems security as well as its collaborative activities with industry, government, and academic organizations.

Abstract

Organizations rely heavily on the use of information technology (IT) products and services to run their day-to-day activities. Ensuring the security of these products and services is of the utmost importance for the success of the organization. This publication provides an introduction to the information security principles organizations may leverage in order to understand the information security needs of their respective systems.

Keywords

assurance; computer security; information security; introduction; risk management; security controls; security requirements

Acknowledgements

The authors would like to thank everyone who took the time to review and make comments on the draft of this publication, specifically Celia Paulsen, Ned Goren, and Isabel Van Wyk of the National Institute of Standards and Technology (NIST). The authors would also like to acknowledge the original authors, Barbara Guttman and Edward A. Roback, as well as all those individuals who contributed to the original version of this publication.

Table of Contents

List of Appendices

List of Figures

1 Introduction

1.1 Purpose

This publication serves as a starting-point for those new to information security as well as those unfamiliar with NIST information security publications and guidelines. The intention of this special publication is to provide a high level overview of information security principles by introducing related concepts and the security control families (as defined in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*) that organizations can leverage to effectively secure their systems. To better understand the meaning and intent of the security control families described later, this publication begins by familiarizing the reader with various information security principles.

After the introduction of these security principles, the publication provides detailed descriptions of multiple security control families as well as the benefits of each control family. The point is not to impose requirements on organizations, but to explore available techniques for applying a specific control family to an organizations system and to explain the benefit(s) of employing the selected controls.

Since this publication serves as an introduction to information security, detailed steps as to how these security controls are implemented or how to check for security control effectiveness are not included. Rather, separate publications that may provide more detailed information about a specific topic will be noted as a reference.

1.2 Intended Audience

The target audience for this publication is those new to the information security principles and tenets needed to protect information and systems in a way that is commensurate with risk. This publication will provide a basic foundation of concepts and ideas to any person tasked with or interested in understanding how to secure systems.

The tips and techniques described in this publication may be applied to any type of information or system in any type of organization. While there may be differences in the way federal organizations, academia, and the private sector process, store, and disseminate information within their respective systems, the basic principles of information security are applicable to all. For that reason, this publication is a good resource for anyone looking to gain a better understanding of information security basics or for those seeking a high level view on the topic.

1.3 Organization

This publication is organized as follows:

- Chapter 1 describes the purpose, target audience, important terms, the legal foundation for information security, and a list of NIST publications related to information security and information risk management.
- Chapter 2 lists eight major elements regarding information security.
- Chapter 3 outlines several roles, supporting roles, and the respective responsibilities attributed to those roles on providing information security to the organization.

- Chapter 4 introduces threats and vulnerabilities, distinguishes the difference between the two, and provides examples of different threat sources and events.
- Chapter 5 discusses information security policy and the differences between Program Policy, Issue-Specific Policy, and System-Specific Policy.
- Chapter 6 considers how to manage risk and briefly describes the six steps of the NIST Risk Management Framework (RMF).
- Chapter 7 focuses on assurance, specifically information assurance, and what measures can be taken to protect information and systems.
- Chapter 8 introduces system support and operations, which collectively function to run a system.
- Chapter 9 provides a brief overview of cryptography as well as several NIST 800-series Publications that contain additional, more detailed information on specific cryptographic technologies.
- Chapter 10 introduces the 17 information security control families as well as the Project Management (PM) family suite of controls.
- Appendix A provides a list of References.
- Appendix B provides a Glossary of terms used throughout the document.
- Appendix C provides a list of Acronyms used throughout the document.

1.4 Important Terminology

The term *Information System* is defined by 44 U.S.C., Sec. 3502 as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." For this publication, the term is used to denote any set of technology used to process data, including hardware, firmware, software, and sensors or other support systems. Some other key terms to be familiar with are[1]:

- Information – (1) Facts or ideas, which can be represented (encoded) as various forms of data; (2) Knowledge (e.g., data, instructions) in any medium or form that can be communicated between system entities.
- Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability.
- Confidentiality – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity – Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.
    - Data Integrity – The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in

[1] These terms and definitions were retrieved from CNSSI 4009, *Committee on National Security Systems (CNSS) Glossary,* dated April 6, 2015.

transit.

  - System Integrity – The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

- Availability – Ensuring timely and reliable access to and use of information.
- Security Controls – The safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

1.5 Legal Foundation for Federal Information Security Programs

Within the Federal Government, a number of laws and regulations mandate that federal departments and agencies protect their systems, the information they process, and related technology resources (e.g., telecommunications). A sampling of these laws and regulations are listed below.

- The *Computer Security Act of 1987* required agencies to identify sensitive systems, conduct computer security training, and develop computer security plans. The *Computer Security Act of 1987* was superseded by the *Federal Information Security Management Act of 2002 (FISMA)*, described below.
- The *Federal Information Resource Management Regulation (FIRMR)* was the primary regulation for the use, management, and acquisition of computer resources in the Federal Government. The law was abolished pursuant to the *Information Technology Management Reform Act of 1996 (ITMRA)*, redesignated the *Clinger-Cohen Act*.
- The *E-Government Act of 2002* is intended to enhance the management and promotion of electronic government services and processes by establishing a Federal Chief Information Officer (CIO) within the Office of Management and Budget (OMB), and by establishing a broad framework of measures that require the use of Internet-based information technology to enhance citizens' access to government information, services, and for purposes.
- The *Federal Information Security Management Act (FISMA)* was enacted as part of the *E-Government Act of 2002* to address specific information security needs, which include, but are not limited to, providing: a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets; and the development and maintenance of minimum controls required to protect federal information and systems (as written in SEC. 301 of Public Law 107-347).
- The *Federal Information Security Modernization Act of 2014* was an amendment to FISMA that made several modifications to modernize federal security practices as well as promote and strengthen the use of continuous monitoring.
- OMB Circular A-130, *Management of Federal Information Resources*, requires that federal agencies establish information security and privacy programs containing specified elements.

- OMB Memo 06-16, *Protection of Sensitive Agency Information*, describes important security controls that agencies can use to protect sensitive agency information and includes a NIST checklist for remote access.
- OMB Memo 04-04, *E-Authentication Guidance for Federal Agencies*, requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance.
- OMB Memo 14-03, *Enhancing the Security of Federal Information and Information Systems*, provides agencies with guidance for managing information security risk on a continuous basis and builds upon efforts to achieve the cybersecurity Cross Agency Priority (CAP) goal.
- OMB Memo 06-15, *Safeguarding Personally Identifiable Information*, directs Senior Officials for Privacy to conduct a review of agency policies and processes and take necessary corrective action to prevent intentional or negligent misuse of, or unauthorized access to, PII.
- OMB Memo 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology, provides* updated guidance for reporting security incidents involving PII.

This is not a comprehensive list of laws and regulations related to federal systems. There are more specific requirements imposed on federal agencies depending on the type of information they store, process, and disseminate. Additionally, some existing laws that affect non-government organizations were not included on this list. Examples of these laws include: The Health Insurance Portability and Accountability (HIPPA) Act, which protects the privacy and security of health information; and The Sarbanes-Oxley (SOX) Act, which provides protections to the general public from accounting errors and fraudulent practices in financial systems.

Federal managers are responsible for familiarizing themselves and complying with applicable legal requirements. However, laws and regulations do not typically provide detailed instructions for protecting information. Instead, they specify broad, flexible requirements such as restricting the availability of personal data to authorized users. For example, OMB Memo 06-16, recommends that departments take specific action(s) to compensate for limited physical security controls applied to information that is removed or accessed from outside of the organization. This publication provides guidance on developing an effective, overall information security approach to meet applicable laws or policies.

1.6 Related NIST Publications

When it comes to information security and risk management, there are a specific set of Federal Information Processing Standards (FIPS) and NIST Special Publications (SPs) that apply. They include:

- FIPS 199 – *Standards for Security Categorization of Federal Information and Information Systems*, lists standards for the categorization of information and systems, which in turn provides a common framework and understanding of expressing security in a way that promotes effective management and consistent reporting.

- FIPS 200 – *Minimum Security Requirements for Federal Information and Information Systems*, specifies minimum security requirements for information and systems that support the executive agencies of the Federal Government as well as a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements.

- SP 800-18 – *Guide for Developing Security Plans for Federal Information Systems*, describes the procedures for developing a system security plan, provides an overview of the security requirements of the system, and describes the controls in place or planned for meeting those requirements.

- SP 800-30 – *Guide for Conducting Risk Assessments*, provides guidance for conducting risk assessments of federal systems and organizations.

- SP 800-34 – *Contingency Planning Guide for Federal Information Systems*, assists organizations in understanding the purpose, process, and format of information system contingency plans (ISCPs) development with practical, real-world guidelines.

- SP 800-37 – *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, provides guidelines for applying the Risk Management Framework to federal systems, to including conducting the activities of security categorization, security control selection and implementation, security control assessment, system authorization, and security control monitoring.

- SP 800-39 – *Managing Information Security Risk: Organization, Mission, and Information System View*, provides guidelines to establish an integrated, organization-wide program for managing information security risk to organizational operations (e.g., mission, functions, image, and reputation), assets, individuals, other organizations, and the Nation resulting from the operation and use of federal systems.

- SP 800-53 – *Security and Privacy Controls for Federal Information Systems and* Organizations, provides guidelines for selecting and specifying security controls for organizations and systems supporting the executive agencies of the Federal Government to meet the requirements of FIPS Publication 200.

- SP 800-53A – *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, provides (i) guidelines for building effective security assessment plans and privacy assessment plans; and (ii) a comprehensive set of procedures for assessing the effectiveness of security controls and privacy controls employed in systems and organizations supporting the executive agencies of the Federal Government.

- SP 800-60 – *Guide for Mapping Types of Information and Information Systems to Security Categories*, assists agencies in consistently mapping security impact levels to types of: (i) information (e.g., privacy, medical, proprietary, financial, contractor sensitive, trade secret, investigation); and (ii) systems (e.g., mission critical, mission support, administrative).

- SP 800-128 – *Guide for Security-Focused Configuration Management of Information Systems*, provides guidance for organizations responsible for managing and administrating the security of federal systems and associated environments of operation.

- SP 800-137 – *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, assists organizations in the development of an ISCM strategy and the implementation of an ISCM program, which provide awareness of threats and vulnerabilities, visibility into organizational assets, and the effectiveness of deployed security controls.

2 Elements of Information Security

This publication addresses eight major elements regarding information security in order for the reader to gain a better understanding of how the security requirements and controls discussed in Chapter 10 support the overall operations of the organization. These eight concepts are:

1. Information security supports the mission of the organization.
2. Information security is an integral element of sound management.
3. Information security protections are implemented so as to be commensurate with risk.
4. Information security responsibilities and accountability are made explicit.
5. System owners have information security responsibilities outside their own organizations.
6. Information security requires a comprehensive and integrated approach.
7. Information security is assessed regularly.
8. Information security is constrained by societal factors.

2.1 Information Security Supports the Mission of the Organization

In Chapter 1, information security was defined as the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. The careful implementation of information security controls is vital to protecting an organization's information assets as well as its reputation, legal position, personnel, and other tangible or intangible assets.

Unfortunately, security is sometimes viewed as thwarting the mission of the organization by imposing poorly selected, burdensome rules and procedures on users, managers, and systems. On the contrary, well-chosen security rules and procedures do not exist for their own sake but are put in place to protect important assets and thereby support the overall organizational mission. In today's environment of malware, IT system breaches, and insider threats, publicized security issues can have dire consequences, especially to profitability and to the reputation of the organization. Private and public sector organizations would be able to improve both profits and services with the appropriate security in place. Security, therefore, is a means to an end and not an end in itself.

To act on this, managers need to understand both their organizational mission and how each system supports that mission. After a system's role has been defined, the security requirements implicit in that role can also be defined. Security can then be explicitly stated in terms of the organization's mission.

The roles and functions of a system may not be constrained to a single organization. In an inter-organizational system, each organization benefits from securing the system. For example, for electronic commerce to be successful, each of the participants requires security controls to protect their resources. However, good security on the buyer's system also benefits the seller; the buyer's system is less likely to be used for fraud, to become unavailable, or to otherwise negatively affect the seller. (The reverse is also true.)

2.2 Information Security is an Integral Element of Sound Management

It is vital for systems and related processes to have the ability to protect information, financial assets, physical assets, and employees, while also taking resource availability into consideration. Since information security risk cannot be completely eliminated, the objective is to find the optimal balance between protecting the information or system and utilizing available resources. Management personnel are ultimately responsible for determining the level of acceptable risk for a specific system and the organization as a whole, taking into account the cost of security controls.

When an organization's information and systems are linked with external systems, management's responsibilities extend beyond organizational boundaries. This may require that management (1) know what general level or type of security is employed on the external system(s), or (2) seek assurance that the external system provides adequate security for the. For example, Cloud Service Providers (CSPs) and cloud supply chain participants may assume the management role for storing, processing, and transmitting organizational information. However, that does not leave the organization[2] free of any security related responsibility. It is up to the organization to ensure that the CSPs and cloud supply chain participants provide an appropriate level of security for the information being stored, processed, and transmitted.

2.3 Information Security is Implemented so as to be Commensurate with Risk

Risk to a system can never be completely eliminated. Therefore, it is crucial to manage risk by striking a balance between the usability and the implementation of security controls. The primary objective of risk management is to implement security protections that are commensurate with risk. Applying unnecessary controls may waste resources and make a systems more difficult to use and maintain. Conversely, not applying controls needed to protect the system may leave it and its information vulnerable to breaches in confidentiality, integrity, and availability, all of which could impede or even halt the mission of the organization.

Federal organizations use categories of high, moderate, and low to identify the impact that a loss of confidentiality, integrity, or availability of information and/or a system may have on the organization's operations and allow them to identify appropriate controls. The accurate categorization of information and systems is integral in determining how to protect information commensurate with risk. Security categories convey the impact that a loss of confidentiality, integrity, or availability may have on the mission of the organization. To determine the impact level of a system, organizations may refer to the guidance in FIPS 199, NIST SP 800-30, and NIST SP 800-60.

An accurate determination of the system impact level results in the selection of an appropriate set of security controls from NIST SP 800-53. Part of this assessment includes the costs to implement and maintain the security controls and the expected security benefits (i.e., risk

[2] An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

reduction) from applying those controls.

Security benefits, however, do have both direct and indirect costs. Direct costs include purchasing, installing, and administering security measures (e.g., access control software or fire-suppression systems). Additionally, security measures can sometimes affect system performance, employee morale, or retraining requirements. In many cases, these additional costs may well exceed the initial cost of the control. Organizational management is responsible for weighing the cost versus benefit of the security control implementation and making risk-based decisions.

2.4 Information Security Roles and Responsibilities are made Explicit

The roles and responsibilities of information system owners, common control providers, information security officers, users, and others are clear and documented. If the responsibilities are not made explicit, holding personnel accountable could be a difficult task.

Documenting information security responsibilities is not dependent on the size of the organization. Even small organizations can prepare a document that states the organizational policy and identifies the information security responsibilities for a system or for the entire organization.

Roles and responsibilities are discussed briefly in Chapter 3 of this publication. For more detailed information, specific to key information security participants, refer to Appendix D of NIST SP 800-37.

2.5 System Owners have Information Security Responsibilities Outside their own Organization

Users of a system are not always located within the boundary of the system they use or have access to. For example, when a system interconnection between two or more systems is in place, information security responsibilities might be shared amongst the participating organizations. When such is the case, the system owners are responsible for sharing the security measures used by the organization to provide confidence to the user that the system is adequately secure and capable of meeting security requirements. In addition to sharing security-related information, managers have a duty to respond to security incidents in a timely fashion in order to prevent damage to the organization, personnel, and other organizations.

2.6 Information Security Requires a Comprehensive and Integrated Approach

Providing effective information security requires a comprehensive approach that considers a variety of areas both within and outside of the information security field. This approach applies throughout the entire information life cycle.

For example, defense in depth is a method used to secure organizational information and systems from malicious activity by using complex, multi-layered security countermeasures. Defense in depth utilizes security technologies such as intrusion detection systems, firewalls, and antivirus software in tandem with physical security defenses (e.g., gates, guards) to minimize the probability of a successful attack on the system. These measures not only help reduce the likelihood that a security breach will compromise access to system assets or have detrimental effects on confidentiality, integrity, or availability, but also give the organization more time to respond once an attack has been detected.

2.6.1 Interdependencies of Security Controls

Security controls are seldom put in place as a stand-alone solution to a problem. They are typically more effective when paired with another control or set of controls. Security controls, when selected properly, can have a synergistic effect on the overall security of a system.

Not understanding these interdependencies can be detrimental to the system. For example, without proper training on how and when to use a virus-detection package, the user may apply the package incorrectly and, therefore, ineffectively. As a result, the user may mistakenly believe that the system will always be virus-free and may inadvertently spread a virus.

2.6.2 Other Interdependencies

Interdependencies between and amongst security controls are not the only factor that can influence the effectiveness of security controls. System management, legal constraints, quality assurance, privacy concerns, and internal and management controls can also affect the functionality of the selected controls. System managers must be able to recognize how information security relates to other security disciplines like physical and environmental security. Understanding how those relationships work together will prove beneficial when implementing a more holistic security strategy. NIST SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, provides much more detailed information of considerations to engineering a trustworthy system.

Understanding the relationships between security controls is especially important when systems are connected to other systems or interconnected to a globally distributed supply chain ecosystem. Supply chains consist of public and private sector entities and use geographically diverse routes to provide a highly refined, cost-effective, reusable information and communications technology (ICT) solution. For more information on supply chain risk management, see NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.

2.7 Information Security is Assessed Regularly

Information security is not a static process and requires continuous monitoring and management to protect the confidentiality, integrity, and availability of information as well as to ensure that new vulnerabilities and evolving threats are quickly identified and responded to accordingly. In the presence of a constantly evolving workforce and technological environment it is essential that organizations provide timely and accurate information while operating at an acceptable level of risk.

Information Security Continuous Monitoring (ISCM) is defined in NIST SP 800-137 as the maintenance of ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. ISCM provides a clear understanding of organizational risk tolerance to assist officials in setting priorities and managing risk throughout the organization in a consistent manor. ISCM ensures that the selected security controls remain effective and maintains organizational awareness of threats and vulnerabilities.

For more detailed information on continuous monitoring fundamentals and the continuous monitoring process, refer to NIST SP 800-137. NIST SP 800-53A can also be leveraged to provide insight on assessment procedures.

2.8 Information Security is Constrained by Societal Factors

Societal factors influence how individuals understand and use systems which consequently impacts the information security of the system and organization. Individuals perceive, reason, and make risk-based decisions in different ways. To address this, organizations make information security functions transparent, easy to use, and understandable. Additionally, providing regularly scheduled security awareness training also mitigates individual differences of risk perception.

It is incumbent on organizations to find a balance between information security requirements and usability. Organizations can leverage a variety of tools that meet the security requirements of their system(s) without unduly burdening the user. For example, consider a system that requires a user to input their username and password multiple times to access different applications during a single session. In that scenario, organizations can choose which types of applications, if any, will permit password and password hash storage based on a consideration of the risks versus the convenience of the users. Privacy was once considered to be unrelated to information security; the two functions were discussed as if they could not co-exist in a system. Today, a symbiotic relationship between privacy and information security is essential. Organizations cannot have effective privacy without a basic foundation of information security. However, privacy is more than security as it also relates to problems that individuals may experience as a result of the authorized processing of their information throughout the data life cycle. Protecting the privacy of individuals is a fundamental responsibility of organizations that collect, use, maintain, share, and dispose of personally identifiable information (PII)[3]. For more detailed privacy information see NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems.*

Overall, the relationship between security and societal norms need not necessarily be antagonistic. Societal norms can have both a positive and negative impact on information security. For example, a negative impact on information security can be seen in the form of a user writing down passwords and keeping them near their computer. A positive impact can be seen by a broader implementation of two factor authentication—where in order for a user to reset a password, more than one form of authentication is required (e.g. text message to user, physical token). Security can enhance the access and flow of data and information by providing more accurate and reliable information as well as greater availability of systems. Security mechanisms can also enhance individuals' privacy (like encryption). There are some security mechanisms

[3] Personally Identifiable Information (PII), as defined in OMB Circular A-130, is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. This definition is broad and extends beyond commonly understood biographical information to include any information that can be linked to an individual, including behavioral or transactional information.

though that may present new risks (like monitoring). Thus, it is important to consider how to implement security solutions in ways that optimize broader societal goals.

Societal norms change and so to must the information security protections placed on systems. Security controls that are presently sufficient will not always keep pace with the constantly changing computing environment. The culture and security environment of the organization also plays an important role in the employees' perception of risk. Insufficient or non-existent security standards will undoubtedly lead to the degradation of the organization's security posture. Providing constant and recurring training on what is and what is not an acceptable use of organizational systems safeguards the overall security of the system.

3 Roles and Responsibilities

The following chapter outlines specific organizational roles and their respective responsibilities. Clearly defined roles and responsibilities help the organization and its employees work in a more efficient manner by designating who is responsible for performing certain tasks. In a large organization, this will help by ensuring that no task is overlooked. In a small, less structured organization, the workload can be more evenly distributed as an employee may be required to take on more than one task.

The list provided below is not intended to be a comprehensive list of all the possible roles within an organization. Each organization may define their own specific roles or have a different naming convention based on their mission or organizational structure. However, the basic functions remain the same. For a more detailed description of the responsibilities assigned to each role, see Appendix D in NIST SP 800-37.

3.1 Risk Executive Function (Senior Management)

The Risk Executive Function is an individual or group (e.g. board members, CEO, CIO) within an organization responsible for ensuring that: (i) risk-related considerations for individual systems are viewed from an organization-wide perspective, taking into consideration the overall strategic goals of the organization in carrying out its core missions and business functions, and (ii) the management of system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success.

Responsibilities include, but are not limited to:

- Defining a holistic approach to addressing risk across the entire organization
- Developing an organization-wide risk management strategy
- Supporting information-sharing amongst authorizing officials and other senior leaders within the organization
- Overseeing risk-management related activities across the organization

3.2 Chief Executive Officer (CEO)

The Chief Executive Officer is the highest-level senior official or executive in an organization with the overall responsibility to provide information security protections commensurate with the risk and magnitude of harm (i.e. impact) to organizational operations assets, individuals, other organizations, and the Nation that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of: (i) information collected or maintained by or on behalf of the agency; and (ii) systems used or operated by an agency, or by a contractor of an agency, or another organization on behalf of an agency.

Responsibilities include, but are not limited to:

- Ensuring the integration of information security management processes with strategic and operational planning processes

- Making sure that the information and systems used to support organizational operations have proper information security safeguards
- Confirming that trained personnel are complying with related information security legislation, policies, directives, instructions, standards, and guidelines

3.3 Chief Information Officer (CIO)

The Chief Information Officer is an organizational official responsible for: (i) designating a senior information security officer; (ii) developing and maintaining security policies, procedures, and control techniques to address all applicable requirements; (iii) overseeing personnel with significant responsibilities for information security and ensuring that personnel are adequately trained; (iv) assisting senior organizational officials with their security responsibilities; and (v) in coordination with other senior officials, reporting annually on the overall effectiveness of the organization's information security program, including progress of remedial actions.

Responsibilities include, but are not limited to:

- Allocating resources dedicated to the protection of the systems supporting the organization's mission and business functions
- Ensuring that systems are protected by approved security plans and are authorized to operate
- Making sure that there is an organization-wide information security program that is being effectively implemented

3.4 Information Owner/Steward

The Information Owner/Steward is an organizational official with statutory, management, or operational authority for specified information who is responsible for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal.

Responsibilities include, but are not limited to:

- Establishing the rules for the appropriate use and protection of the subject information
- Providing input to system owners regarding the security requirements and security controls for their system(s)

3.5 Senior Information Security Officer (SISO)

The Senior Information Security Officer is an organizational official responsible for: (i) carrying out the chief information officer security responsibilities under FISMA; and (ii) serving as the primary liaison between the chief information officer and the organization's authorizing officials, system owners, common control providers, and information security officers. In some organizations, this role might also be known as the Chief Information Security Officer (CISO).

Responsibilities include, but are not limited to:

- Assuming the role of authorizing official designated representative or security control assessor when needed

3.6 Authorizing Official (AO)

The Authorizing Official is a senior official or executive with the authority to formally assume responsibility for operating a system at an acceptable level of risk to organizational operations and assets, individuals, and other organizations.

Responsibilities include, but are not limited to:

- Approving security plans, memorandums of agreement or understanding, plans of action and milestones, as well as determining whether significant changes in the system or environments of operation require reauthorization
- Ensuring that authorizing official designated representatives carry out all activities and functions associated with security authorization.

3.7 Authorizing Official Designated Representative

The Authorizing Official Designated Representative is an organizational official who acts on behalf of an authorizing official to coordinate and conduct the required day-to-day activities associated by the security authorization process. The designated representative carries out the functions of the AO, but cannot accept risk for the system.

Responsibilities include, but are not limited to:

- Carrying out the duties of the Authorizing Official as assigned
- Making certain decisions with regard to the planning and resourcing of the security authorization process, approval of the security plan, approving and monitoring the implementation of plans of action and milestones, and the assessment and/or determination of risk
- Preparing the final authorization package, obtaining the authorizing official's signature on the authorization decision document, and transmitting the authorization package to appropriate organizational officials

3.8 Senior Agency Official for Privacy (SAOP)

The Senior Agency Official for Privacy is a senior organizational official who has the overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act. The SAOP Responsibilities include, but are not limited to:

- Overseeing, coordinating, and facilitating the agency's compliance efforts
- Reviewing the agency's information privacy procedures to ensure that they are comprehensive and up-to-date
- Ensure the agency's employees and contractors receive appropriate training and education programs regarding the information privacy laws, regulations, policies, and procedures governing the agency's handling of personal information.

3.9 Common Control Provider

The Common Control Provider is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (i.e. security controls inherited by systems).

Responsibilities include, but are not limited to:

- Documenting the organization-identified common controls in a security plan (or equivalent document prescribed by the organization)
- Ensuring that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence defined by the organization

3.10 Information System Owner

The Information System Owner is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system.

Responsibilities include, but are not limited to:

- Addressing the operational interests of the user community (i.e., users who require access to the system to satisfy mission, business, or operational requirements)
- Ensuring compliance with information security requirements
- Developing and maintaining the security plan and ensuring that the system is deployed and operated in accordance with the agreed-upon security controls

3.11 Information Security Officer (ISO)

The Information Security Officer is responsible for ensuring that an appropriate operational security posture is maintained for a system and as such, works in close collaboration with the information system owner.

Responsibilities include, but are not limited to:

- Overseeing the day-to-day security operations of a system
- Assisting in the development of the security policies and procedures and to ensuring compliance with those policies and procedures

3.12 Information Security Architect

The Information Security Architect is an individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution models, and the resulting systems supporting those missions and business processes.

Responsibilities include, but are not limited to:

- Serving as the liaison between the enterprise architect and the information security engineer
- Coordinating with information system owners, common control providers, and information security officers on the allocation of security controls as system-specific, hybrid, or common controls

3.13 Information Security Engineer (ISE)

The Information Security Engineer is an individual, group, or organization responsible for conducting system security engineering activities.

Responsibilities include, but are not limited to:

- Designing and developing organizational systems or upgrading legacy systems
- Coordinating security-related activities with information security architects, senior information security officers, information system owners, common control providers, and information security officers

3.14 Security Control Assessor

The Security Control Assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of the managerial, operational, and technical security controls and control enhancements employed within or inherited by a system to determine the overall effectiveness of the controls (i.e. 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).

Responsibilities include, but are not limited to:

- Providing an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation
- Recommending corrective actions to address identified vulnerabilities
- Preparing the final security assessment report containing the results and findings from the assessment

3.15 System Administrator

The System Administrator is an individual, group, or organization responsible for setting up and maintaining a system or specific components of a system.

Responsibilities include, but are not limited to:

- Installing, configuring, and updating hardware and software
- Establishing and managing user accounts
- Overseeing backup and recovery tasks

3.16 User

The User is an individual, group, or organization granted access to organizational information in order to perform the duties specifically assigned to them.

Responsibilities include, but are not limited to:

- Adhering to policies that govern acceptable use of organizational systems
- Using the organization-provided IT resources for defined purposes only
- Reporting anomalies or suspicious system behavior

3.17 Supporting Roles

- *Audit*. Auditors are responsible for examining systems to determine: (i) whether the system is meeting stated security requirements and organization policies; and (ii) whether security controls are appropriate. Informal audits can be performed by those operating the system under review or by impartial third-party auditors.

- *Physical Security*. The physical security office is responsible for developing and enforcing appropriate physical security controls, often in consultation with information security management, program and functional managers, and others. Physical security addresses central system installations, backup facilities, and office environments. In the government, this office is often responsible for processing personnel background checks and security clearances.

- *Disaster Recovery/Contingency Planning Staff*. Some organizations have a separate disaster recovery/contingency planning staff. In such cases, the staff is typically responsible for contingency planning for the organization as a whole and work with program and functional mangers/application owners, the information security staff, and others to obtain additional contingency planning support, as needed.

- *Quality Assurance*. Many organizations have established a quality assurance program to improve the products and services they provide to their customers. The quality officer should have a working knowledge of information security and how it can be used to enhance the quality of the program (e.g. ensuring the integrity of computer-based information, the availability of services, and the confidentiality of customer information).

- *Procurement*. The procurement office is responsible for ensuring that organizational procurements have been reviewed by appropriate officials. While the procurement office lacks the technical expertise to guarantee that goods and services meet information security expectation it should nevertheless be knowledgeable of information security standards and should bring them to the attention of those requesting such technology.

- *Training Office*. The organization determines whether the primary responsibility for training users, operators, and managers in information security rests with the training office or the information security program office. In either case, the two organizations should work together to develop an effective training program.

- *Human Resources.* The Human Resource office is often the first point-of-contact for managers who require assistance in determining whether or not a security background investigation is necessary for a particular position. The personnel and security offices generally work closely on issues involving background investigations. The personnel office may also be responsible for explaining security-related exit procedures when employees leave an organization.

- *Risk Management/Planning Staff.* Some organizations employ a full-time staff devoted to analyzing all manner of risks to which the organization may be exposed. Although this office normally focuses on “macro” issues, it should also consider information security-related risks. Risk analyses for specific systems are not typically performed by this office.

- *Physical Plant.* This office is responsible for ensuring the provision of the services necessary for the safe and secure operation of an organization's systems (e.g. electrical power and environmental controls). The office is often augmented by separate medical, fire, hazardous waste, or life safety personnel.

- *Privacy*. This office is responsible for maintaining a comprehensive privacy program that ensures compliance with applicable privacy requirements, develops and evaluates privacy policy, and manages privacy risks. This office includes a Senior Authorizing Official for Privacy, privacy compliance and risk assessment specialists, legal specialists, and other professionals focused on managing privacy risks, and particularly with respect to this publication those that may arise from information security measures.

4 Threats and Vulnerabilities: A Brief Overview

Vulnerabilities leave systems susceptible to a multitude of activities that can result in significant and sometimes irreversible losses to an individual, group, or organization. These can range from a single damaged file on a laptop to entire databases at an operations center being compromised. With the right tools and knowledge, an adversary can exploit system vulnerabilities and gain access to the information stored on them. The damage inflicted on compromised systems can vary depending on the threat source.

A threat source can be adversarial or non-adversarial. Adversarial threat sources are individuals, groups, organizations, or states that seek to exploit an organization's dependence on cyber resources. Even employees, privileged users, and trusted users have been known to defraud organizational systems. Non-adversarial threat sources refer to natural disasters or erroneous actions taken by individuals in the course of executing their everyday responsibilities.

Threat sources can lead to threat events. A threat event is an incident or situation that could potentially cause undesirable consequences or impacts. An example of a threat source leading to a threat event would be a hacker installing a keystroke monitor on an organizational system. The damage that these vulnerabilities can cause on systems varies considerably. Some affect the confidentiality and integrity of the information stored in a system while others only affect the availability of the system. For more information on threat sources and threat events, see NIST SP 800-30.

This chapter presents a broad overview of the environment in which systems operate today and may prove valuable to organizations seeking a better understanding of their specific threat environment. The list provided herein is not intended to be an all-inclusive list. The scope of the information provided here may be too broad, and threats against specific systems could be quite different from what is discussed in this chapter.

In order to protect a system from risk and to implement the most cost-effective security measures, information system owners, managers, and users need to know and understand the vulnerabilities of the system as well as the threat sources and events that may exploit them. If a vulnerability exists, but there is no threat to take advantage of it, little or nothing is gained by expending resources to correct that vulnerability. See Chapter 6, *Information Security Risk Management*, for more detailed information on how threats, vulnerabilities, safeguard selection and risk mitigation are related.

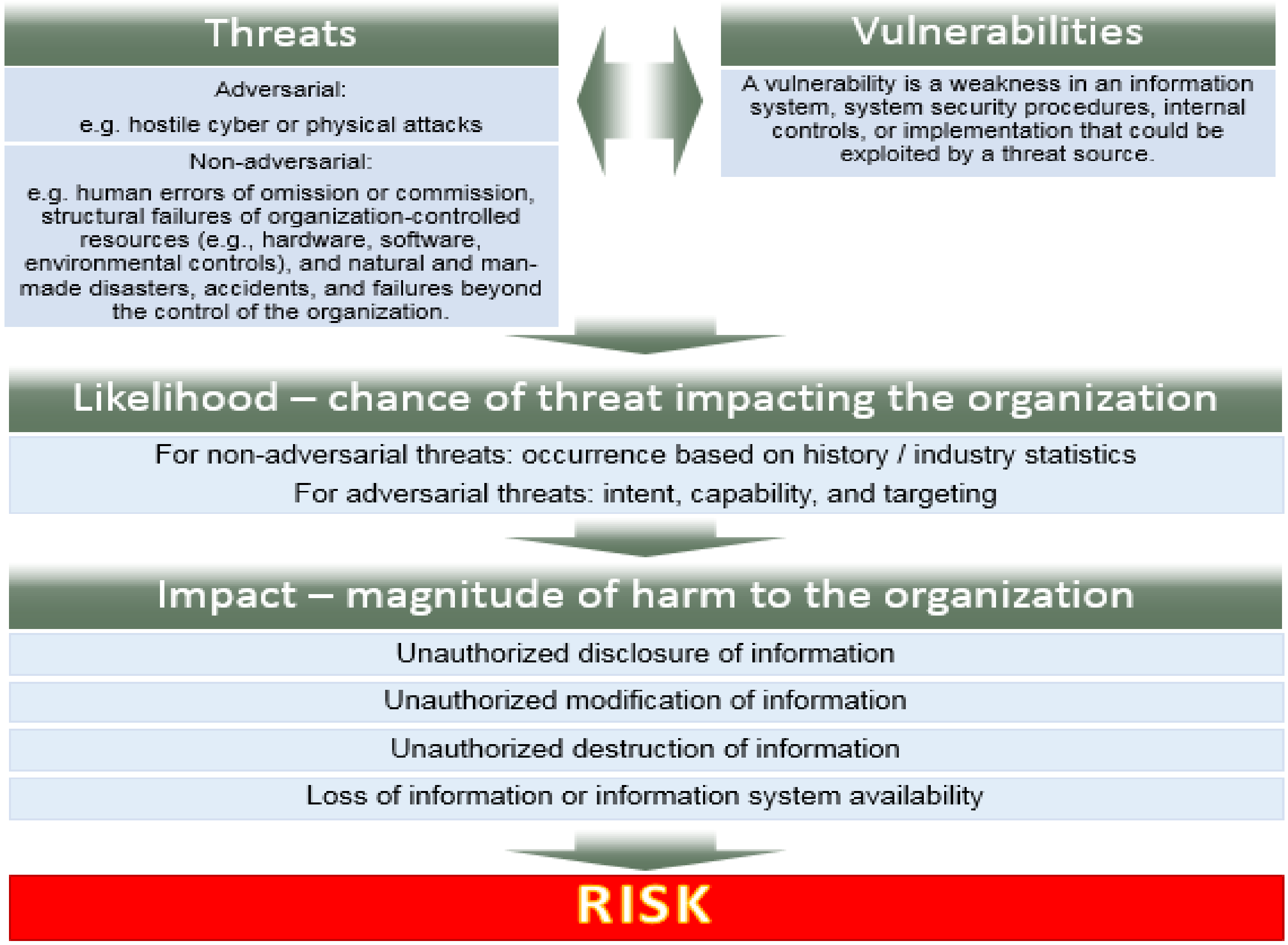

Figure 1 - Risk Assessment Model

4.1 Examples of Adversarial Threat Sources and Events

The previous section defined threat sources and threat events. This section provides several examples of each followed by a description.

4.1.1 Fraud and Theft

Systems can be exploited for fraud and theft by “automating” traditional methods of fraud or by utilizing new methods. System fraud and theft can be committed by insiders (i.e. authorized users) and outsiders. Authorized system administrators and users with access to and familiarity with the system (e.g. resources it controls, flaws) are responsible for the majority of fraud. An organization’s former employees also pose a threat given their knowledge of the organization’s operations particularly if their access is not terminated promptly.

It has been successfully proven that individuals were able to skim small amounts of money from a large number of financial accounts. Financial gain is one of the chief motivators behind fraud and theft, but financial systems are not the only systems at risk. There are several techniques that an individual can use to gather information they would otherwise not have had access to. Some of these techniques include:

- *Social Media.* The ubiquity of social media has allowed cyber criminals to exploit the platform in order to conduct targeted attacks. Using easily-made, fake, and unverified social media accounts, cyber criminals can impersonate co-workers, customer service representatives, or other trusted individuals in order to send malware links that steal personal or sensitive organizational information. Social media exacerbates the ongoing issue of fraud, and organizations should see it is a serious concern when implementing systems.

- *Social Engineering.* Social engineering, in the context of information security, is a technique that relies heavily on human interaction to influence an individual to violate their normal security protocol and encourages the individual to divulge confidential information. These types of attacks are commonly committed via phone or online. Attacks perpetrated over the phone are the most basic social engineering attacks being committed. For example, an attacker will fool a company into believing they are a customer and have that company divulge information about the customer they are impersonating. Online, this technique is called phishing–an attack intended to trick individuals into revealing login credentials, passwords, or other personal information. Social engineering online attacks can also be accomplished by the use of attachments that contain malware, which target an individual's address book. The information obtained allows the attacker to send the malicious file to all of the contacts in that person's address book, propagating the damage of the initial attack.

- *Advanced Persistent Threat (APT).* An advanced persistent threat is a long-term, covert attack that often employs a social engineering technique to gain access to a network. To maintain access, the attacker constantly rewrites the code to avoid being discovered by an intrusion detection system (IDS). Once enough information about the network has been gathered, the attacker can create a back door, which is a way of bypassing security mechanisms in systems, and gain undetected access to the network. An external command and control system is then used by the attacker to continuously monitor the system to extract information.

4.1.2 Insider Threat

Employees can represent an insider threat to an organization given their familiarity with the employer's systems and applications as well as what actions may cause the most damage, mischief, or disorder. Employee sabotage—often instigated by knowledge or threat of termination—is a critical issue for organizations and their systems. In an effort to mitigate the potential damage caused by employee sabotage, the terminated employee's access to IT infrastructure should be immediately disabled, and the individual should be escorted off company premises.

Examples of system-related employee sabotage include:

- Destroying hardware or facilities
- Planting logic bombs that destroy programs or data

- Entering data incorrectly, holding data, or deleting data
- Crashing systems

4.1.3 Malicious Hacker

Malicious hacker is a term used to describe an individual or group who use an advanced understanding of systems, networking, and programming to illegally access systems, cause damage, or steal information. Understanding the motivation that drives a malicious hacker can help an organization implement the proper security controls to prevent the likelihood of a system breach. Malicious hacker is a broad category of adversarial threats that can be broken out into smaller categories depending on the specific actions or intent of the malicious hacker. Some of the sub-categories described in NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security,* include:

- *Attackers.* Attackers break into networks for the thrill and challenge or for bragging rights in the attacker community. While remote hacking once required considerable skills or computer knowledge, attackers can now download attack scripts and protocols from the Internet and launch them against victim sites. These attack tools have become both more sophisticated and easier to use. Many attackers do not have the requisite expertise to threaten difficult targets such as critical government networks. Nevertheless, the worldwide population of attackers poses a relatively high threat of isolated or brief disruptions that could cause serious damage to business or infrastructure.

- *Bot-Network Operators.* Bot-network operators assume control of multiple systems to coordinate attacks and distribute phishing schemes, spam, and malware. The services of compromised systems and networks can be found in underground markets online (e.g., purchasing a denial of service attack, using servers to relay spam or phishing attacks).

- *Criminal Groups*. Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups use spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose threats to the Nation based on their ability to conduct industrial espionage, large-scale monetary theft, and the recruitment of new attackers. Some criminal groups may try to extort money from an organization by threatening a cyber-attack.

- *Foreign Intelligence Services*. Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrines, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power – impacts that could affect the daily lives of U.S. citizens.

- *Insiders*. The disgruntled insider is a principal source of computer crime. Insiders may not require in-depth knowledge of computer intrusions because their knowledge of a target system often allows them unrestricted access to cause damage to the system or to steal system data. Insiders may be employees, contractors, business partners, or outsourced vendors who accidentally introduce malware into systems.

Inadequate policies, procedures, and testing can—and have—led to ICS impacts. Impacts have ranged from trivial to significant damage to the ICS and field devices. Unintentional impacts from insiders represent some of the highest probability occurrences.

- *Phishers*. Phishers are individuals or small groups that execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
- *Spammers*. Spammers are individuals or organizations that distribute unsolicited e-mail with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (e.g., DoS).
- *Spyware/Malware Authors*. Individuals or organizations who maliciously carry out attacks against users by producing and distributing spyware and malware. Destructive computer viruses and worms have that harmed files and hard drives include the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
- *Terrorists*. Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware to generate funds or gather sensitive information. They may also attack one target to divert attention or resources from other targets.
- *Industrial Spies*. Industrial espionage seeks to acquire intellectual property and know-how using clandestine methods.

4.1.4 Malicious Code

Malicious code refers to viruses, Trojan horses, worms, logic bombs, and any other foreign software that can be used to attack a platform.

- *Virus*. A code segment that replicates by attaching copies of itself to existing executables. The new copy of the virus is executed when a user executes the new host program. The virus may include an additional "payload" that triggers when specific conditions are met. For example, some viruses display a text string on a particular date. There are many types of viruses, including variants, overwriting, resident, stealth, and polymorphic.
- *Trojan Horse*. A program that performs a desired task, but that also includes unexpected and undesirable functions. For example, consider an editing program for a multiuser system. This program could be modified to randomly and unexpectedly delete a user’s files each time they perform a useful function (e.g. editing).
- *Worm*. A self-replicating program that is self-contained and does not require a host program or user intervention. Worms commonly use network services to propagate to other host systems.

- *Logic Bomb*. This type of malicious code is a set of instructions secretly and intentionally inserted into a program or software system to carry out a malicious function at a predisposed time and date or when a specific condition is met.

4.1.5 Foreign Government Espionage

In some instances, threats posed by foreign government intelligence services may be present. In addition to possible economic espionage, foreign intelligence services may target unclassified systems to further their intelligence missions. Some unclassified information that may be of interest includes travel plans of senior officials, civil defense and emergency preparedness, manufacturing technologies, satellite data, personnel and payroll data, and law enforcement, investigative, and security files.

4.2 Examples of Non-Adversarial Threat Sources and Events

4.2.1 Errors and Omissions

Errors and omissions can be inadvertently caused by system operators who process hundreds of transactions daily or by users who create and edit data on organizational systems. These errors and omissions can degrade data and system integrity. Software applications, regardless of the level of sophistication, are not capable of detecting all types of input errors and omissions. Therefore, it is the responsibility of the organization to establish a sound awareness and training program to reduce the number and severity of errors and omissions.

Errors by users, system operators, or programmers may occur throughout the life cycle of a system and may directly or indirectly contribute to security problems. In some cases, the error is a threat, such as a data entry error or a programming error that crashes a system. In other cases, the errors cause vulnerabilities. Programming and development errors, often referred to as “bugs,” can range from benign to catastrophic.

4.2.2 Loss of Physical and Infrastructure Support

The loss of supporting infrastructure includes power failures (e.g., outages, spikes, brownouts), loss of communications, water outages and leaks, sewer malfunctions, disruption of transportation services, fire, flood, civil unrest, and strikes. A loss of infrastructure often results in system downtime in unexpected ways. For example, employees may not be able to get to work during a winter storm, although the systems at the work site may be functioning as normal. Additional information can be found in section 10.11, *Physical and Environmental Protection.*

4.2.3 Impacts to Personal Privacy of Information Sharing

The accumulation of vast amounts of PII by government and private organizations has created a number of opportunities for individuals to experience privacy problems as a byproduct or unintended consequence of a breach in security. For example, migrating information to a cloud server has become a viable option that many individuals and organizations utilize. The ease of accessing data from the cloud has made it a more attractive solution for long term storage. Everything that is written, uploaded, or posted is stored in a cloud server that individuals do not control. However, unbeknownst to the cloud service user, personal information can be accessed by a stranger with the right tools and technical skill sets.

Individuals' increased, voluntary sharing of PII through social media has also contributed to new threats that allow malicious hackers to use that information for social engineering or to bypass common authentication measures. Linking all of this information and technology together, malicious hackers with criminal intentions have the ability to create accounts using someone else's information or gain access to networks.

Organizations may share information about cyberthreats that includes PII. These disclosures could lead to unanticipated uses of such information, including surveillance or other law enforcement actions.

5 Information Security Policy

The term policy has more than one definition when discussing information security. NIST SP 800-95, *Guide to Secure Web Services,* defines policy as "statements, rules or assertions that specify the correct or expected behavior of an entity." For example, an authorization policy might specify the correct access control rules for a software component. The term policy can also refer to specific security rules for a particular system or even the specific managerial decisions that dictate an organization's e-mail privacy policy or remote access security policy.

Information security policy is defined as an aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information. In making these decisions, managers face difficult decisions with regard to resource allocation, competing objectives, and organizational strategy, all of which relate to protecting technical and information resources as well as guiding employee behavior. Managers at all levels make choices that can affect policy, with the scope of the policy's applicability varying according to the scope of the manager's authority.

Managerial decisions on information security issues vary greatly. To differentiate various kinds of policy, this chapter categorizes them into three basic types: Program Policy, Issue-specific Policy, and System-specific Policy.

Policy controls are addressed by the -1 controls for every security control family found in NIST SP 800-53. The -1 controls establish policy and procedures for the effective implementation of the selected security control and control enhancement.

5.1 Standards, Guidelines, and Procedures

Because policy is written at a broad level, organizations also develop standards, guidelines, and procedures that offer users, managers, and others a clearer approach to implementing policy and meeting organizational goals. Standards and guidelines specify technologies and methodologies to be used to secure systems. Procedures are yet more detailed steps to be followed to accomplish particular security-related tasks. Standards, guidelines, and procedures may be promulgated throughout an organization via handbooks, regulations, or manuals.

Organizational standards (not to be confused with American National Standards, FIPS, Federal Standards, or other national or international standards) specify uniform use of specific technologies, parameters, or procedures when such uniform use will benefit an organization. Standardization of organization-wide identification badges is a typical example, providing ease of employee mobility and automation of entry/exit systems. Standards are normally compulsory within an organization.

Guidelines assist users, systems personnel, and others in effectively securing their systems. The nature of guidelines, however, immediately recognizes that systems vary considerably, and imposition of standards is not always achievable, appropriate, or cost-effective. For example, an organizational guideline may be used to help develop system-specific standard procedures. Guidelines are often used to help ensure that specific security measures are not overlooked, although they can be implemented, and correctly so, in more than one way.

Procedures normally assist in complying with applicable security policies, standards, and guidelines. They are detailed steps to be followed by users, system operations personnel, or others to accomplish a particular task (e.g. preparing new user accounts and assigning the appropriate privileges).

Some organizations issue overall information security manuals, regulations, handbooks, or similar documents. These may mix policy, guidelines, standards, and procedures, since they are closely linked. While manuals and regulations can serve as important tools, it is often useful if they clearly distinguish between policy and its implementation. This can help in promoting flexibility and cost-effectiveness by offering alternative implementation approaches to achieving policy goals.

5.2 Program Policy

Program policy is used to create an organization's information security program. Program policies set the strategic direction for security and assign resources for its implementation within the organization. A management official—typically the SISO/CISO—issues program policy to establish or restructure the organization's information security program. This high-level policy defines the purpose of the program and its scope within the organization, addresses compliance issues, and assigns responsibility to the information security organization for direct program implementation as well as other related responsibilities.

5.2.1 Basic Components of Program Policy

Program policy addresses the following:

- *Purpose*. Program policy often includes a statement describing the purpose and goals of the program. Security-related needs such as integrity, availability, and confidentiality can form the basis of organizational goals established in the policy. For instance, in an organization responsible for maintaining large mission-critical databases, a reduction in errors, data loss, data corruption, and recovery might be specifically stressed. However, in an organization responsible for maintaining confidential personal data, goals might emphasize stronger protection against unauthorized disclosure.
- *Scope*. Program policies are clear as to which resources (e.g., facilities, hardware and software, information, and personnel) the information security program protects. In many

cases, the program will encompass all systems and organizational personnel, while in others, it might be appropriate for an organization's information security program to be more limited in scope. For example, a policy intended to protect information stored on a classified or high impact system will be much more stringent than that of a policy intended to secure a system deemed to be low impact.

- *Responsibilities*. Once the information security program is established, its management is normally assigned to either a newly created or existing office. The responsibilities of officials and offices throughout the organization also need to be addressed. This section of the policy statement, for example, would distinguish between the responsibilities of information service providers and the managers of applications using the provided services. The policy would also establish operational security offices for major systems, particularly those at high risk or that are most critical to organizational operations. It can also serve as the basis for establishing employee accountability. Role and responsibilities were addressed in Chapter 3 of this publication.
- *Compliance*. Program policy typically addresses two compliance issues:
  1. General compliance to ensure meeting the requirements to establish a program and the responsibilities assigned therein to various organizational components. Often an oversight (e.g. the Inspector General) is assigned responsibility for monitoring compliance, including how well the organization is implementing management's priorities for the program.
  2. The use of specified penalties and disciplinary actions. Since the security policy is a high-level document, specific penalties for various infractions are not normally detailed here. Instead, the policy may authorize the creation of compliance structures that include violations and specific disciplinary actions.

An important aspect of developing compliance policy is to remember that an employee's violation of policy may be unintentional. For example, nonconformance can often be to the result of a lack of knowledge or training. The need to obtain guidance from appropriate legal counsel is critical when addressing issues involving penalties and disciplinary action for individuals. The policy does not need to restate penalties already addresses by law, although they can be listed if the policy will also be used as an awareness or training document.

5.3 Issue-Specific Policy

Based on the guidance from the information security policy, issue-specific policies are developed to address areas of current relevance and concern to an organization. The intent is to provide specific guidance and instructions on proper usage of systems to employees within the organization. An issue-specific policy is meant for every technology the organization uses and is written in such a way that it will be clear to users. Unlike program policies, issue-specific policies must be reviewed on a regular basis due to frequent technological changes in an organization.

5.3.1 Example Topics for Issue-Specific Policy

There are many areas for which issue-specific policy may be appropriate. New technologies and the discovery of new threats often require the creation of an issue-specific policy. Examples of issue-specific policy include:

- *Internet Access*. Connecting to the Internet yields many benefits as well as many problems. Some issues an Internet access policy may address include identifying who will have access, what types of systems may be connected to the network, what types of information may be transmitted via the network, requirements for user authentication for Internet-connected systems, and the use of firewalls.
- *E-mail Privacy*. This policy will clarify what information is collected and stored and the way the information is being used. Management may wish to monitor the employee to ensure that they are only using organizational systems for business purposes, or to determine if the employee is distributing viruses, sending offensive email, or disclosing private business information. Users may be accorded a certain level of privacy in regard to email, and this policy addresses what level of privacy they can expect as well as the circumstances under which their e-mail may be read.
- *Bring Your Own Device (BYOD)*. Allows individuals to use their personal devices in the workplace. Allowing BYOD can increase productivity and decrease costs to the organization. However, introducing different operating systems and user configurations to the organizations network can be challenging, not only to the security of the organizations information, but also to the privacy of the employee. A comprehensive BYOD policy will have specific considerations for the device and the user as well as rules of behavior which must be adhered to in order to access organizational resources using personal devices.
- *Social Media*. Even if the organization does not have a social media presence, chances are their users will. Having a social media policy is crucial for protecting the organization and its employees. A social media policy provides guidelines for users that delineate expected behavior when using different social media platforms. Depending on the organization, the policy can be strict—not allowing the use of social media on organization provided resources—or a lenient policy that allows social media access within organization specified limitations.

Other topics that are candidates for issue-specific policy include, but are not limited to: approach to risk management and contingency planning, protection of confidential/proprietary information, unauthorized software, unauthorized use of equipment, violations of policy, use of external storage, rights of privacy, and physical emergencies.

5.3.2 Basic Components of Issue-Specific Policy

An issue-specific policy can be broken down into the following components:

- *Issue statement.* To formulate a policy on an issue, information owner/steward first define the issue with any relevant terms, distinctions, and conditions included. It is often useful to specify the goal or justification for the policy in an effort to ensure compliance. For example, an organization might want to develop an issue-specific policy on the use of "unofficial software," which might be defined to mean any software not approved, purchased, screened, managed, or owned by the organization. Additionally, the applicable distinctions and conditions might then need to be included for some software, such as that for software privately owned by employees but approved for use at work, or owned and used by other businesses under contract to the organization.

- *Statements of the Organization's Position.* Once the issue is stated and related terms and conditions are discussed, this section is used to clearly state the organization's position (i.e., management's decision) on the issue. To continue the previous example, this would mean stating whether the use of unofficial software as defined is prohibited in all or some cases, whether there are further guidelines for approval and use, or whether case-by-case exceptions will be granted, by whom, and on what basis.
- *Applicability*. Issue-specific policies also need to include statements of applicability. This means clarifying where, how, when, to whom, and to what a particular policy applies. For example, it could be that the hypothetical policy on unofficial software is intended to apply only to the organization's own on-site resources and employees and not to contractors with offices at other locations. Additionally, the policy's applicability might need to be clarified as it pertains to employees travelling among different sites, working from home, or who need to transport and use disks at multiple sites.
- *Roles and Responsibilities*. The assignment of roles and responsibilities is also usually included in issue-specific policies. For example, if the policy permits employees to use privately owned, unofficial software at work with the appropriate approvals, then the approval authority granting such permission would need to be stated. (Policy would stipulate, who, by position, has such authority.) Likewise, it would need to be clarified who would be responsible for ensuring that only approved software is used on organizational system resources and, possibly, for monitoring users in regard to unofficial software.
- *Compliance*. For some types of policy, it may be appropriate to describe unacceptable infractions and the consequences of such behavior in greater detail. Penalties may be explicitly stated and consistent with organizational personnel policies and practices. When used, they can be coordinated with appropriate officials, offices, and even employee bargaining units. It may also be desirable to task a specific office in the organization with monitoring compliance.
- *Points of Contact and Supplementary Information*. For any issue-specific policy, indicate the appropriate individuals to contact in the organization for further information, guidance, and compliance. Since positions tend to change less often than the individuals occupying them, specific positions may be preferable as the point of contact. For example, for some issues the point of contact might be a line manager; for other issues it might be a facility manager, technical support person, system administrator, or security program representative. Using the above example once more, employees would need to know whether the point of contact for questions and procedural information would be their immediate superior, a system administrator, or an information security official.

5.4 System-Specific Policy

Program and issue-specific policies are broad, high-level policies written to encompass the entire organization where system-specific policies provide information and direction on what actions are permitted on a particular system. These policies are similar to issue-specific policies in that they relate to specific technologies throughout the organization. However, system-specific policies dictate the appropriate security configurations to the personnel responsible for implementing the required security controls in order to meet the organization's information security needs.

To develop a cohesive and comprehensive set of security policies, officials may use a management process that derives security rules from security goals. It is helpful to consider a two-level model for system security policy: security objectives and operational security rules. Closely linked and often difficult to distinguish, however, is the implementation of the policy in technology. Similar to issue-specific policies, it is recommended that system-specific policies be reviewed frequently to ensure conformance to the most current security procedures.

5.4.1 Security Objectives

The first step in the management process is to define security objectives commensurate with risk for the specific system. Although this process may begin with an analysis of the need for integrity, confidentiality, and availability, it may not stop there. A security objective needs to be specific, concrete, well defined, and stated in such a way that it is a clearly achievable objective. Stakeholders play an important role in developing comprehensive yet practical policy. Therefore, it is imperative to remember that policy is not created by management personnel only.

5.4.2 Operational Security Rules

After management determines the security objectives, rules for managing and operating a system can be identified and documented. For example, the rules may define authorized modifications—specifying individuals allowed to take certain actions under particular conditions with regard to specific classes and records of information. The degree of specificity needed for operational security vary from system-to-system. The more detailed the rules are, the easier it is for administrators to determine when a violation has occurred. A detailed description can also streamline automating policy enforcement.

In addition to deciding the level of detail, management determines the degree of formality in documenting the system-specific policy. Once again, the more formal the documentation, the easier it is to enforce and to follow the policy. For example, a helpful practice would be to draft a statement of the access privileges for a system as well as the assignment of security responsibilities. The rules for system usage and the consequences of noncompliance should also be addressed. Documenting access controls policy can make it substantially easier to follow and to enforce.

Policy decisions in other areas of information security, such as those described in this publication, are often documented in the risk analysis, accreditation statements, or procedural manuals. However, any controversial, atypical, or uncommon policies will also need formal statements. Atypical policies may include areas in which the system policy varies from organizational policy or from normal practice within the organization. The documentation for a typical policy contains a statement explaining the reason for deviation from the organization's standard policy.

5.4.3 System-Specific Policy Implementation

Technology plays an important role in enforcing system-specific policies but it is not solely responsible for meeting an organization's security needs. When technology is used to enforce policy, it is important to consider nontechnology-based methods. For example, technical system-based controls could be used to limit the printing of confidential reports to a particular printer. However, corresponding physical security measures would also have to be in place to limit access to the printer output or the desired security objective would not be achieved.

Technical methods frequently used to implement system-security policy are likely to include the use of logical access controls. Some examples of access controls would be: separation of duties, which is a control designed to address the potential for abuse of authorized privileges and helps reduce the risk of malevolent activity without collusion; and least privilege, which allows only authorized access for users or processes acting on behalf of users that is necessary to accomplish assigned tasks in accordance with organizational missions and business functions. However, there are other automated means of enforcing or supporting security policy that typically supplement logical access controls. For example, technology intrusion detection software can alert system administrators to suspicious activity or even take action to stop such activity.

Technology-based enforcement of system-security policy has both advantages and disadvantages. A system, properly designed, programmed, installed, configured, and maintained, consistently enforces policy within the system, although no system can force users to follow all procedures. Management controls also play an important role in policy enforcement, so neglecting them would be detrimental to the organization. In addition, deviations from the policy may sometimes be necessary and appropriate; such deviations may be difficult to implement easily with some technical controls. This situation occurs frequently if implementation of the security policy is too rigid, which can occur when the system analysts fail to anticipate contingencies and prepare for them.

5.5 Interdependencies

Policy is related to many of the topics covered in this publication:

- *Program Management*. Policy is used to establish an organization's information security program and is therefore closely tied to program management and administration. Both program and system-specific policy may be established in any of the areas covered in this publication. For example, an organization may wish to have a consistent approach to contingency planning for all its systems and would issue appropriate program policy to do so. On the other hand, it may decide that its systems are sufficiently independent of each other that system owners can deal with incidents on an individual basis.
- *Access Controls*. System-specific policy is often implemented through the use of access controls. For example, it may be a policy decision that only two individuals in an organization are authorized to run a check-printing program. Access controls are used by the system to implement or enforce this policy.
- *Links to Broader Organizational Policies*. This chapter has focused on the types and components of information security policy. However, it is important to understand that

information security policies are often extensions of organizational policies in other forms (e.g., paper documents). For example, an organization's email policy would likely be relevant to its broader policy on privacy. Information security policies may also be extensions of other policies, such as those regarding the appropriate use of equipment and facilities.

5.6 Cost Considerations

A number of potential costs are associated with developing and implementing information security policies. The most significant costs are implementing the policy and addressing its subsequent impacts on the organization, its resources, and personnel. The establishment of an information security program, accomplished through policy, does not come at negligible cost.

Other costs may be those incurred through the policy development process. Numerous administrative and management activities may be required for drafting, reviewing, coordinating, clearing, disseminating, and publicizing policies. In many organizations, successful policy implementation may require additional staffing and training. In general, the costs to an organization for information security policy development and implementation will be dependent upon how extensive the change must be in order for management to decide that an acceptable level of risk has been reached.

The cost of securing information and systems is unavoidable. The objective is to ensure that security protections are commensurate with risk by striking a balance between the protections required to meet the security objectives of the organization and the cost of such protections.

6 Information Security Risk Management

Risk is a measure of the extent an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Individuals manage risks every day, though they may not be aware of it. Actions as routine as buckling a car safety belt, carrying an umbrella when rain is forecasted, or writing down a list of things to do rather than trusting to memory all fall under the purview of risk management. Individuals recognize various threats to their best interests and take precautions to guard against them or to minimize their effects.

Both government and industry routinely manage a myriad of risks. For example, to maximize their return on investments, businesses must often choose between growth investment plans that are aggressive and high-risk or slow and secure. These decisions require analysis or risk relative to potential benefits, consideration of alternatives, and, finally, the implementation of what management determines to be the best course of action.

With respect to information security, risk management is the process of minimizing risks to organizational operations (e.g., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation of a system. NIST SP 800-39 identifies four distinct steps for risk management. Risk management requires organizations to (i) frame risk, (ii) assess risk, (iii) respond to risk, and (iv) monitor risk.

(i) Risk Framing – describes how organizations establish a risk context for the environment in which risk-based decisions are made. The purpose of the risk framing component is to produce a risk management strategy that addresses how organizations intend to assess, respond to, and monitor risk—while making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions.

(ii) Assessing Risk – describes how organizations analyze risk within the context of the organizational risk frame. The purpose of the risk assessment component is to identify: (i) threats to organizations (i.e., operations, assets, or individuals) or threats directed at organizations or the Nation; (ii) internal and external vulnerabilities of organizations; (iii) the harm (i.e., consequences/impact) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur.

(iii) Responding to Risk – addresses how organizations respond to risk once that risk is determined based on the results of risk assessments. The purpose of the risk response component is to provide a consistent, organization-wide response to risk in accordance with the organizational risk frame by: (i) developing alternative courses of action for responding to risk; (ii) evaluating the alternative courses of action; (iii) determining appropriate courses of action consistent with organizational risk tolerance; and (iv) implementing risk responses based on selected courses of action.

(iv) Monitoring Risk – addresses how organizations monitor risk over time. The purpose of the risk monitoring component is to: (i) verify that planned risk response measures are implemented and that information security requirements derived from/traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, standards, and guidelines are satisfied; (ii) determine the ongoing effectiveness of risk response measures following implementation; and (iii) identify risk-impacting changes to organizational systems and the environments in which the systems operate.

To help organizations manage information security risk at the system level, NIST developed the Risk Management Framework (RMF). The RMF promotes the concept of near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes. The RMF also provides senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational systems supporting their core missions and business functions, and integrates information security into the enterprise architecture and system development life cycle. The six steps that comprise the RMF include:

1. Security Categorization
2. Security Control Selection
3. Security Control Implementation
4. Security Control Assessment
5. System Authorization
6. Security Control Monitoring

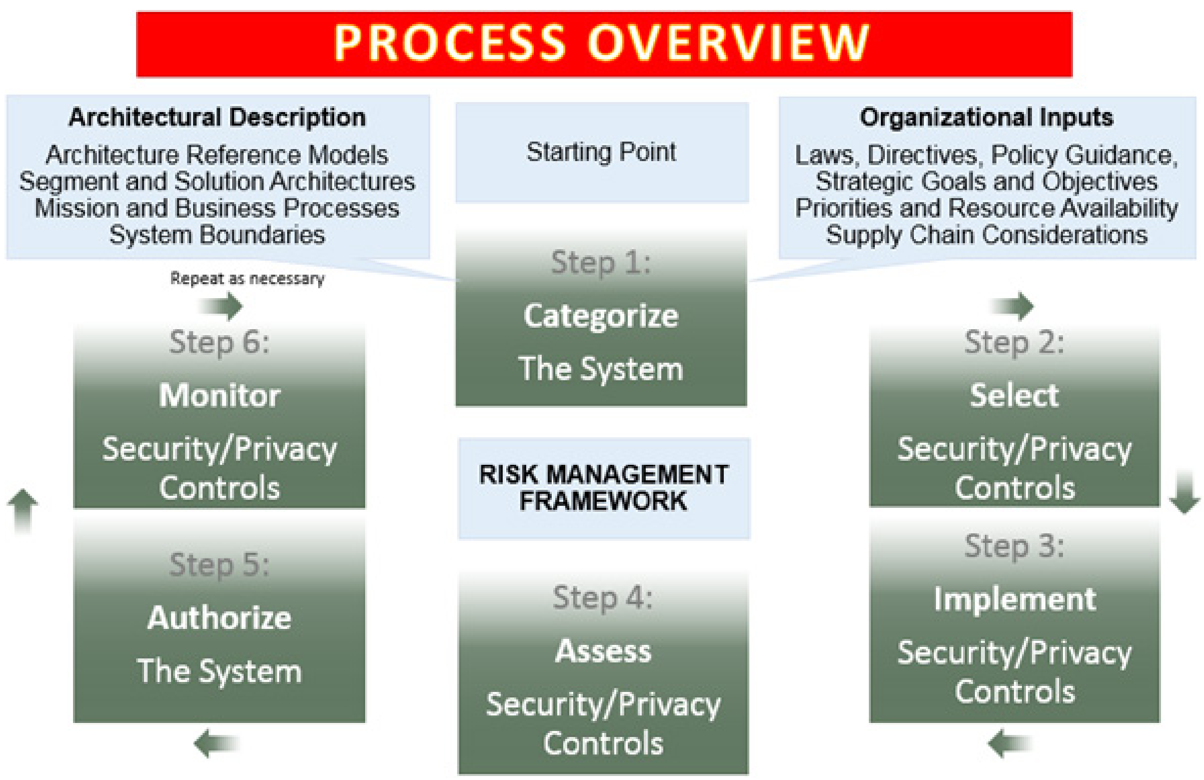

Figure 2 - Risk Management Framework (RMF) Overview

6.1 Categorize

The first step of the RMF focuses on the categorization of the system. Here, organizations categorize the system and the information processed, stored, and transmitted by that system based on an impact analysis. Security categorization guidance for non-national security systems can be found in FIPS 199 and NIST SP 800-60.

6.2 Select

The second step of the RMF process involves selecting an initial set of baseline security controls for the system based on the security categorization as well as tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions. Security control selection guidance is provided in NIST SP 800-53 and in FIPS 200.

6.3 Implement

In the third step, the organization is responsible for implementing security controls and describing how the controls are employed within the system and its environment of operation. Many NIST publications with information on security control implementation are available for reference on the Computer Security Resource Center website.

6.4 Assess

The fourth step ensures that the organization assesses the security controls using appropriate assessment procedures and 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. NIST SP 800-53A provides guidelines for the development of assessment methods and procedures to determine security control effectiveness in federal systems and for reporting assessment findings in the security assessment report.

6.5 Authorize

In the fifth step, management officially authorizes a system to operate or continue to operate based on the results of a complete and thorough security control assessment. This decision is based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the system and the decision that this risk is acceptable.

6.6 Monitor

The sixth step of the RMF is to continuously monitor the security controls in the system to ensure that they are effective over time as changes occur in the system and the environment in which the system operates. Organizations monitor the security controls in the system on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. Specific guidance on continuous monitoring can be found in NIST SP 800-137.

7 Assurance

Information assurance is the degree of confidence one has that security measures protect and defend information and systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of systems by incorporating protection, detection, and reaction capabilities.

Assurance is not, however, an absolute guarantee that the measures will work as intended. Understanding this distinction is crucial as quantifying the security of a system can be daunting. Nevertheless, it is something individuals expect and obtain, often without realizing it. For example, an individual may routinely receive product recommendations from colleagues but may not consider such recommendations as providing assurance.

This chapter discusses planning for assurance and presents two categories of assurance methods and tools: the design and subsequent implementation of assurance and operational assurance (further categorized into audits and monitoring). The division between the two categories can be ambiguous at times as there is significant overlap. While such issues as configuration management or audits are discussed under operational assurance, they may also be vital during a system's development. The discussion tends to focus more on technical issues during design and implementation assurance and is a mixture of management, operational, and technical issues under operational assurance.

7.1 Authorization

Authorization is the official management decision to authorize the operation of a system. The authorizing official (a senior organizational executive) explicitly accepts the risk of operating the system to organizational operations (e.g., mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. There is a need for a collaborative relationship between the authorizing official and the SAOP. OMB A-130 gives SAOPs review and approval of privacy plans prior to authorization, and review of authorization packages for systems with PII. Therefore, before making risk determination and acceptance decisions, the authorizing official communicates with the SAOP to address any privacy related concerns before the final authorization decision is made. The authorization process requires managers and technical staff to work together to find practical, cost-effective solutions given security needs, technical and operational constraints, requirements of other system quality attributes such as privacy, and mission or business requirements.

To facilitate sound risk-based decision making, decisions are based on reliable and current information about the implementation and effectiveness of both technical and nontechnical safeguards. These include:

- Technical features (Do they operate as intended?)
- Operational policies and practices (Is the system operated according to stated policies and practices?)
- Overall security (Are there threats that the safeguards do not address?)

- Remaining risk (Is residual risk[4] at an acceptable level?)

The Authorizing Official is responsible for authorizing the system before it is allowed to operate and have a plan in place for how that system will be continuously monitored.

7.1.1 Authorization and Assurance

Assurance is an integral element in making the decision to authorize a system to operate. Assurance addresses whether the technical measures and procedures are operating according to a set of security requirements and specifications as well as general quality principles.

7.1.2 Selecting Assurance Methods

The authorizing official makes the final decision on how much and what types of assurance are needed for a system. In order to make a sound decision, the authorizing official considers the system categorization/impact level and reviews the results of risk assessments. The authorizing official analyzes the benefits and disadvantages of the cost of assurance, cost of controls, and risks to the organization. When the authorization process is complete, it is the responsibility of the authorizing official to accept the residual risk in the system.

7.1.3 Authorization of Products to Operate in Similar Situation

The authorization of another product or system to operate in a similar situation can be used to provide some assurance. However, it is important to realize that an authorization is specific to the environment and the system. Since authorization balances risks and advantages, the same product may be appropriately authorized for one environment but not for another, even by the same authorizing official. For instance, an authorizing official might approve the use of cloud storage for research data but not for human resource data under the purview of the same system.

7.2 Security Engineering

The size and complexity of today's systems make building a trustworthy system a priority. Systems security engineering provides an elementary approach for building dependable systems in today's complex computing environment. For more information on security engineering, refer to NIST SP 800-160.

7.2.1 Planning and Assurance

For new systems or for system upgrades, assurance requirements begin during the planning phase of the system life cycle. Planning for assurance as part of system requirements also is practical and helps authorizing officials make cost-effective decisions when building a system or when purchasing the components/equipment required to provide assurance for an older system.

[4] Residual Risk is the portion of risk remaining after security measures have been applied.

7.2.2 Design and Implementation Assurance

Design and implementation assurance addresses a system's design as well as whether the features of a system, application, or component meet security requirements and specifications. Design and implementation assurance examines system design, development, and installation and is usually associated with the development/acquisition and implementation phase of the system life cycle. However, it may also be considered throughout the life cycle as the system is modified.

7.2.2.1 Use of Advanced or Trusted Development

In the development of both commercial off-the-shelf (COTS) products and customized systems, the use of advanced or trusted system architectures, development methodologies, or software engineering techniques can provide assurance. Examples include security design and development reviews, formal modeling, mathematical proofs, ISO 9000 quality techniques, ISO 15288 a systems engineering standard, or the use of security architecture concepts, such as a trusted computing base (TCB) or reference monitor.

Since assurance in information technology products cannot be fully guaranteed, there are recognized evaluation processes available to establish a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet certain requirements. Common Criteria (CC) allows for the comparability of results between independent evaluations. CC is useful as a guide for the development, evaluation, and procurement of IT products with security functionality. For more information about CC, see http://www.commoncriteriaportal.org or https://buildsecurityin.us-cert.gov/articles/best-practices/requirements-engineering/the-common-criteria.

7.2.2.2 Use of Reliable Architecture

Some system architectures are intrinsically more reliable, such as systems that use fault-tolerance, redundancy, shadowing, or redundant array of inexpensive disks (RAID) features. These examples are primarily associated with system availability.

7.2.2.3 Use of Reliable Security

One factor in reliable security is the concept of ease of safe use, which postulates that a system that is easier to secure is more likely to actually *be* secure. Security features may be more likely utilized when the initial system defaults to the "most secure" option. In addition, a system's security may be deemed more reliable if it refrains from using new technology that has yet to be tested in the "real" world (often called "bleeding-edge" technology). Conversely, a system that uses older, well-tested software may be less likely to contain bugs.

7.2.2.4 Evaluations

A product evaluation normally includes testing. Evaluations can be performed by many types of organizations, including: domestic and foreign government agencies; independent organizations such as trade and professional organizations; other vendors or commercial groups; or individual users or user consortia. Product reviews in trade literature are a form of evaluation, as are more formal reviews made against specific criteria. Important factors to consider when using evaluations are the degree of independence of the evaluating group, whether the evaluation criteria reflect needed security features, the rigor of the testing, the testing environment, the age of the evaluation, the competence of the evaluating organization, and the limitations placed on the evaluations by the evaluating group (e.g., assumptions about the threat or operating environment).

7.2.2.5 Assurance Documentation

The ability to describe security requirements and how they were met can reflect the degree to which a system or product designer understands applicable security issues. Without a comprehensive understanding of the requirements, it is unlikely that the designer will be able to meet them.

Assurance documentation can address the security for a system or for specific components. System-level documentation describes the system's security requirements and how they have been implemented, including interrelationships among applications, the operating system, or networks. System-level documentation addresses more than just the operating system, the security system, and applications; it describes the system as integrated and implemented in a particular environment. Component documentation will generally be an off-the-shelf product, whereas the system designer or implementer will typically develop system documentation.

7.2.2.6 Warranties, Integrity Statements, and Liabilities

Warranties are an additional source of assurance. A manufacturer, producer, system developer, or integrator that is willing to correct errors within certain time frames or by the next release, gives the system manager a sense of commitment to the product and also speaks to the product’s quality. An integrity statement is a formal declaration or certification of the product. It can be augmented by a promise to (a) fix the item (i.e., warranty) or (b) pay for losses (i.e., liability) if the product does not conform to the integrity statement.

7.2.2.7 Manufacturer’s Published Assertions

The published assertion or formal declarations of a manufacturer or developer provide a limited amount of assurance based on reputation. When there is a contract in place, reputation alone will be insufficient given the legal liabilities imposed on the manufacturer.

7.2.2.8 Distribution Assurance

It is often important to know that software has arrived unmodified, especially if it is distributed electronically. In such cases, check bits or digital signatures can provide high assurance that code has not been modified. Anti-virus software can be used to check software that comes from sources with unknown reliability (e.g., internet forum).

7.3 Operational Assurance

Design and implementation assurance addresses the quality of security features built into systems. Operational assurance addresses whether the system's technical features are being bypassed or have vulnerabilities and whether required procedures are being followed. It does not address changes in the system's security requirements, which could be caused by changes to the system and its operating or threat environment. (These changes are addressed in section 10.15).

Security tends to degrade during the operational phase of the system life cycle. System users and operators discover new ways to intentionally or unintentionally bypass or subvert security, especially if there is a perception that bypassing security improves functionality or that there will be no repercussions to them or their systems. Strict adherence to procedures is rare. Policy becomes outdated, and errors in the system's administration commonly occur.

Organizations use three basic methods to maintain operational assurance:

- *System assessment*. An event or a continuous process to evaluate security. An assessment can vary widely in scope: it may examine an entire system for the purpose of authorization or it may investigate a single anomalous event.
- *System audit*. An independent review and examination of records and activities to assess the adequacy of system controls and to ensure compliance with established policies and operational procedures.
- *System monitoring*. A process for maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

In general, the more "real-time" an activity is, the more it falls into the category of monitoring. This distinction can create some unnecessary linguistic hairsplitting, especially concerning system generated audit trails. Daily or weekly reviewing of the audit trail for unauthorized access attempts is generally considered to be monitoring, while a historical review of several months' worth of the trail (e.g., tracing the actions of a specific user) is generally considered an audit. Overall, though, the specific terms applied to assurance-related activities are much less important than the real work of actually maintaining operational assurance.

7.3.1 Assessments

Assessments can address the quality of the system as built, implemented, or operated. Assessments can be performed throughout the development cycle, after system installation, and throughout its operational phase. Assessment methods include interviews, examinations, and testing. Some common testing techniques feature functional testing (to see if a given function works according to its requirements) or penetration testing (to see if security can be bypassed). These techniques can range from trying several test cases to in-depth studies using metrics, automated tools, or multiple detailed test cases. See NIST SP 800-53A for assessment guidance.

7.3.2 Audit Methods and Tools

An audit conducted to support operational assurance examines whether the system is meeting stated or implied security requirements as well as system and organization policies. Some audits also examine whether security requirements are appropriate, though this is outside of the scope of operational assurance. (See section 10.15.) Less formal audits are often called security reviews.

Audits can be self-administered or independent (either internal or external). Both types can provide excellent information about technical, procedural, managerial, or other aspects of security. The essential difference between a self-audit and an independent audit is objectivity. Reviews conducted by system management staff—often called self-audits/assessments—present an inherent conflict of interest. The system management staff may have little incentive to report that the system was poorly designed or is carelessly operated. On the other hand, they may be motivated by a strong desire to improve the security of their system. In addition, they are knowledgeable about the system and may be able to find hidden problems.

The independent auditor, by contrast, has no professional stake in the system. A person who performs an independent audit is organizationally independent and free from personal or external constraints that may impair their independence. An independent audit may be performed by a professional audit staff in accordance with generally accepted auditing standards.

There are numerous methods and tools that can be used to audit, some of which are described here. Several of them overlap.

7.3.2.1 Automated Tools

Even for small multiuser systems, manually reviewing security features may require significant resources. Automated tools make it feasible to review even large systems for a variety of security flaws.

There are two types of automated tools: (1) active tools, which find vulnerabilities by trying to exploit them; and (2) passive tests, which only examine the system and infer the existence of problems from the state of the system.

Automated tools can be used to help uncover a variety of threats and vulnerabilities, such as improper access controls or access control configurations, weak passwords, lack of system software integrity, or not using all relevant software updates and patches. These tools are often very successful at finding vulnerabilities and are sometimes used by hackers to break into systems. Not taking advantage of these tools puts system administrators at a disadvantage. Many of the tools are simple to use. However, some programs (e.g., access-control auditing tools for large mainframe systems) require specialized skill to use and interpret.

7.3.2.2 Internal Controls Audit

An auditor can review controls in place and determine whether they are effective. The auditor will often analyze both system and non-system based controls. Techniques used include inquiry, observation, and testing of both the data and the controls themselves. The audit can also detect illegal acts, errors, irregularities, or a lack of compliance with laws and regulations. System Security Plans and penetration testing, discussed below, may be used.

7.3.2.3 Using the System Security Plan (SSP)

The system security plan provides implementation details against which the system can be audited. This plan, discussed in section 10.12, outlines the major security considerations for a system, including management, operational, and technical issues. One advantage of using a system security plan is that it reflects the unique security environment of the system, rather than a generic list of controls. Security control sets can be developed, including national or organizational security policies and practices (often referred to as baselines). The SSP is also used for historical purposes and, in such instances where a system interconnection exists, may need to be shared with other organizations.

Baselines are the starting point of the security control selection process for systems. Three security control baselines have been identified corresponding to the low-impact, moderate-impact, and high-impact systems using the high water mark[5] defined in FIPS 200 to provide an initial set of security controls for each impact level. Once a security control baseline is selected, organizations use the tailoring guidance in NIST SP 800-53 to remove controls from the baseline (with a justification based on risk) or to add compensating or supplemental controls to strengthen the security posture of a specific system.

Care needs to be taken to ensure that deviations from the baseline are based on an assessment of the associated risk as the changes may be appropriate for the system's particular environment or technical constraints.

7.3.2.4 Penetration Testing

Penetration testing can use many methods to attempt a system break-in. In addition to using active automated tools as described above, penetration testing can be done "manually." The most useful type of penetration testing involves the use of methods that might actually be used against the system. For hosts on the Internet, this would certainly include automated tools. For many systems, lax procedures or a lack of internal controls on applications are common vulnerabilities that penetration testing can target. Another method is social engineering, which involves deceiving users or administrators into divulging information about systems, including their passwords.

7.3.3 Monitoring Methods and Tools

Security monitoring is an ongoing activity that seeks out vulnerabilities and security problems. Many of the methods are similar to those used for audits but are done more regularly or, for some automated tools, in real time.

7.3.3.1 Review of System Logs

A periodic review of system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours (see section 10.15).

[5] High Water Mark—For a system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values from among those security categories that have been determined for each type of information resident on the system (retrieved from FIPS 199).

7.3.3.2 Automated Tools

Several types of automated tools monitor a system for security problems. Some examples follow:

- Virus scanners are a popular means of checking for virus infections. These programs test for the presence of viruses in executable program files.
- Check-sums presume that program files are not changed between updates. They work by generating a mathematical value based on the contents of a particular file. When the integrity of the file is being verified, the checksum is generated on the current file and compared with the previously generated value. If the two values are equal, the integrity of the file is verified. Running check-sums on programs can detect viruses, Trojan horses, accidental changes to files caused by hardware failures, and other changes to files. However, they may be subject to covert replacement by a system intruder. Digital signatures can also be used.
- Password strength checkers test passwords against a dictionary (either a "regular" dictionary or a specialized one with easy-to-guess passwords) and also check if passwords are common permutations of the user ID. Examples of special dictionary entries could be the names of regional sports teams and stars. Common permutations could be the user ID spelled backwards. System administrators can use this tool to measure the strength of users’ passwords.
- Integrity verification programs can be used by applications to look for evidence of data tampering, errors, and omissions. Techniques include consistency and reasonableness checks and validation during data entry and processing. These techniques can check data elements—as input or as processed—against expected values or ranges of values; analyze transactions for proper flow, sequencing, and authorization; or examine data elements for expected relationships. Integrity verification programs comprise a crucial set of processes meant to assure individuals that inappropriate actions, whether accidental or intentional, will be caught. Many integrity verification programs rely on logging individual user activities.
- Intrusion detectors analyze the system audit trail for activity that could represent unauthorized activity, particularly logons, connections, operating systems calls, and various command parameters. Intrusion detection is covered in sections 10.1 and 10.3.
- System performance monitoring analyzes system performance logs in real time to look for availability problems, including active attacks, system and network slowdowns, and crashes.
- EINSTEIN is a system managed by the Department of Homeland Security (DHS) that provides monitoring for a specified set of security controls and issues across the federal civilian executive branch. EINSTEIN helps manage information security risk by detecting and blocking attacks from compromising federal agencies as well as by providing DHS with situational awareness of threat information detected on one system to help protect other systems within the Government and private sector.

7.3.3.3 Configuration Management

Configuration management provides assurance that the system in operation has been configured to organizational needs and standards, that any changes to be made are reviewed for security implications, and that such changes have been approved by management prior to implementation. Configuration management can be used to help ensure that changes take place in an identifiable and controlled environment and that they do not unintentionally harm any of the system's properties, including its security. Some organizations, particularly those with very large systems (e.g., the Federal Government), use a configuration control board for configuration management. When such a board exists, it is crucial for an information security expert to participate.

Changes to the system can have security implications. Such changes may introduce or mitigate vulnerabilities and may require updating the contingency plan, risk analysis, or authorization. For more details on configuration management, see section 10.5.

7.3.3.4 Trade Literature/Publications/Electronic News

In addition to monitoring the system, it is useful to monitor external sources for information. Such sources as trade literature, both printed and electronic, have information about security vulnerabilities, patches, and other areas that impact security. The Forum of Incident Response Teams (FIRST) has an electronic mailing list that receives information on threats, vulnerabilities, and patches. The National Vulnerability Database (NVD) is a repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. Also, the United States Computer Emergency Readiness Team (US-CERT), a DHS component, responds to major incidents, analyzes threats, and exchanges critical cybersecurity information with trusted partners around the world

7.4 Interdependencies

Assurance is an issue for every control and safeguard discussed in this publication. Are user IDs and access privileges kept up to date? Has the contingency plan been tested? Can the audit trail be tampered with? One important point to reemphasize here is that assurance is not only for technical controls but for operational controls as well. Although the chapter focused on systems assurance, it is also important to have assurance that management controls are working properly. Is the security program effective? Are policies understood and followed? As noted in the introduction to this chapter, the need for assurance is more widespread than individuals often realize.

Assurance is closely linked to planning for security in the system life cycle. Systems can be designed to facilitate various kinds of testing against specified security requirements. By planning for such testing early in the process, costs can be reduced. In some certain cases, some kinds of assurance cannot be obtained without proper planning.

7.5 Cost Considerations

There are many methods of obtaining assurance that security features work as anticipated. Since assurance methods tend to be qualitative rather than quantitative, they will need to be evaluated. Assurance can also be quite expensive, especially if extensive testing is done. It is useful to evaluate the amount of assurance received for the cost to make a best-value decision. In general, personnel costs drive up the cost of assurance. Automated tools are generally limited to addressing specific problems, but they tend to be less expensive.

8 Security Considerations in System Support and Operations

System support and operations refers to all aspects involved in running a system. This includes both system administration and tasks external to the system that support its operation (e.g., maintaining documentation). It does not include system planning or design. The support and operation of any system—from a three-person local area network to a worldwide application serving thousands of users—is critical to maintaining the security of a system. Support and operations are routine activities that enable systems to function correctly. These include fixing software or hardware problems, installing and maintaining software, and helping users resolve problems.

The failure to consider security as part of the support and operations of systems, can be detrimental to the organization. Information security system literature includes examples of how organizations undermined their often expensive security measures with poor documentation, old user accounts, conflicting software, or poor control of maintenance accounts. An organization's policies and procedures often fail to address many of these important issues. Some major categories include:

- User support
- Software support
- Configuration management
- Backups
- Media controls
- Documentation
- Maintenance

Even though the goals of system support and operation and information security are closely related, there is a distinction between the two. The primary goal of system support and operations is the continued and correct operation of the system, whereas the information security goals of a system include confidentiality, availability, and integrity.

This chapter addresses the support and operations activities directly related to security. Every control discussed in this publication relies, in one way or another, on system support and operations. However, this chapter, focuses on areas not covered in other chapters. For example, operations personnel normally create user accounts on the system. This topic is covered in section 10.7 so is therefore not discussed here. Similarly, the input from support and operations staff to the security awareness and training program is covered in section 10.2.

8.1 User Support

In many organizations, user support takes place through a Help Desk. Help Desks can support an entire organization, a subunit, a specific system, or a combination of these. For smaller systems, the system administrator typically provides direct user support. Experienced users provide informal user support on most systems. It is not unusual for user support to be closely linked to the organization's ability to handle incident response.

An important security consideration for user support personnel is being able to recognize which problems (brought to their attention by users) are security-related. For example, users' inability to log on to a system may result from the disabling of their accounts due to too many failed access attempts. This could indicate the presence of malicious users trying to guess a user's password.

In general, system support and operations staff need to be able to identify security problems, respond accordingly, and inform appropriate individuals. A wide range of possible security problems may exist; some will be internal to custom applications, while others apply to off-the-shelf products. Additionally, problems can be software- or hardware-based.

The more responsive and knowledgeable system support and operation staff personnel are; the less user support will be provided informally. The support other users provide can be valuable, but they may not be aware of all the issues across the organization or how they are related.

8.2 Software Support

Software is the heart of an organization's system operations, whatever the size and complexity of the system. Therefore, it is essential that software function correctly and be protected from corruption. There are many elements of software support.

The first element is controlling what software is used on a system. If users or systems personnel can install and execute any software on a system, the system is more vulnerable to viruses, unexpected software interactions, and software that may subvert or bypass security controls. One method of controlling software is to inspect or test software before it is installed (e.g., determine compatibility with custom applications, identify other unforeseen interactions). This can apply to new software packages, upgrades, off-the-shelf products, or to custom software, as deemed appropriate. In addition to controlling the installation and execution of new software, organizations also oversee the configuration and use of powerful system utilities. System utilities can compromise the integrity of operating systems and logical access controls.

The second element in software support can be to ensure that software has not been modified without proper authorization. This involves the protection of software and backup copies and can be done with a combination of logical and physical access controls.

Many organizations also include a program to ensure that software is properly licensed, as required. For example, an organization may audit systems for illegal copies of copyrighted software. This problem is primarily associated with PCs and LANs, but can apply to any type of system.

8.3 Configuration Management

Closely related to software support is configuration management—the process of tracking and approving changes to the system. Configuration management can be formal or informal and normally addresses hardware, software, networking, and other changes. The primary security goal of configuration management is to ensure that changes to the system do not unintentionally or unknowingly diminish security. Some of the methods discussed under software support (e.g., such as inspecting and testing software changes) can be used. Chapter 7 discusses other methods.

Note that the security goal is to know what changes occur, not to prevent security from being changed. There may be circumstances under which reducing security is deemed an acceptable risk due to the need to accomplish the mission. In such cases, the decrease in security is based on a decision by the authorizing official who considered all appropriate factors. Furthermore, the resulting increase in risk is monitored on an ongoing basis.

A second security goal of configuration management is to ensure that changes to the system are reflected in other documentation, such as the contingency plan. If the change is major, it may be necessary to reanalyze some or all of the security of the system. This is discussed in section 10.15.

8.4 Backups

Support and operations personnel and sometimes users back up software and data. This function is critical to contingency planning. The frequency of backups depends on how often data changes and how important those changes are. Consult with system administrator to determine what backup schedule is appropriate. Also, it is important to test that backup copies are actually usable. Finally, store backups securely (discussed below).

8.5 Media Controls

Media controls include a variety of measures to provide physical and environmental protection and accountability for digital and non-digital media. Example of digital media include diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Examples of non-digital media include paper and microfilm. From a security perspective, media controls are designed to prevent the loss of confidentiality, integrity, or availability of information, including data or software, when stored or disseminated outside of the system. This can include storage of information before it is input into the system and after it is output.

The extent of media control depends on many factors, including the type of data, the quantity of media, and the nature of the user environment. Physical and environmental protection is used to prevent unauthorized individuals from accessing the media and protects against such factors as heat, cold, or harmful magnetic fields. When necessary, logging the use of individual media (e.g., a tape cartridge) provides detailed accountability –so that the organizations may hold authorized individuals responsible for their actions. For more information on media protection, see section 10.10.

8.6 Documentation

Documentation of all aspects of system support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations are performed correctly and efficiently.

The specific security implementation details of a system are also documented. This includes many types of documentation, such as security plans, contingency plans, risk analyses, and security policies and procedures. Much of this information, particularly risk and threat analyses, has to be protected against unauthorized disclosure. Security documentation also needs to be both current and accessible. Accessibility takes special factors into consideration such as the need to find the contingency plan during a disaster.

Some security documentation may need to be designed to fulfill the needs of different system roles. For this reason, many organizations separate documentation into policy and procedures. A security procedures manual may be written to inform system users on how to do their jobs securely. For systems operations and support staff, a security procedures manual may address a wide variety of technical and operational concerns in considerable detail.

8.7 Maintenance

System maintenance requires either physical or logical access to the system. Support and operations staff, hardware or software vendors, or third-party service providers may maintain a system. Maintenance may be performed on-site or remotely via communications connections. It may also be necessary to move equipment to a repair site for maintenance. If someone who does not typically have access to the system performs maintenance, then a security vulnerability is introduced.

In some circumstances, it may be necessary to take additional precautions (e.g., background investigation of service personnel) to prevent some problems such as "snooping around" the physical area. However, once someone has access to the system, it is very difficult for supervision to prevent damage done through the maintenance process.

Many systems provide maintenance accounts. These special login accounts are normally preconfigured at the factory with pre-set, widely known passwords. It is critical to change these passwords or otherwise disable or block/limit access to the accounts until they are needed. Develop procedures to ensure that only authorized maintenance personnel have access to the preconfigured accounts. If the account is to be used remotely, authentication of the maintenance provider can be performed using call-back confirmation. This helps ensure that remote diagnostic activities actually originate from an established phone number at the vendor's site. Other helpful techniques include encryption and decryption of diagnostic communications, strong identification and authentication techniques such as tokens, and remote disconnect verification.

Manufacturers of larger systems and third-party providers may offer more diagnostic and support services, and larger systems may have diagnostic ports. It is critical to ensure that these ports are only used by authorized personnel and cannot be accessed by malicious users.

8.8 Interdependencies

There are support and operations components in most of the controls discussed in this publication

- *Personnel*. Most support and operations staff have special access to the system. Some organizations conduct background checks on individuals in these positions. (See section 10.13).

- *Incident Handling.* Support and operations may include an organization's incident handling staff. Even if they are separate organizations, they need to work together to recognize and respond to incidents. (See section 10.8).
- *Contingency Planning*. Support and operations normally provides technical input to contingency planning and carries out the activities of creating backups, updating documentation, and practicing responses to contingencies. (See section 10.6).
- *Security Awareness, Training, and Education*. Support and operations staff are trained in security procedures and aware of the importance of security. In addition, they provide technical expertise needed to teach users how to secure their systems. (See section 10.2).
- *Physical and Environmental*. Support and operations staff often control the immediate physical area around the system. (See section 10.11).
- *Technical Controls*. The technical controls are installed, maintained, and used by support and operations staff. They create the user accounts, add users to access control lists, review audit logs for unusual activity, control bulk encryption over telecommunications links, and perform the countless operational tasks needed to use technical controls effectively. In addition, support and operations staff provide needed input to the selection of controls based on their knowledge of system capabilities and operational constraints.
- *Assurance*. Support and operations staff ensure that changes to a system do not introduce security vulnerabilities by using assurance methods to evaluate or test the changes and their effects on the system. Operational assurance is normally performed by support and operations staff. (See Chapter 7).

8.9 Cost Considerations

The cost of ensuring adequate security in day-to-day support and operations is largely dependent upon the size and characteristics of the operating environment and the nature of the processing being performed. It is usually not necessary to hire additional support and operations security specialists. If sufficient support personnel are already available, it is important that they be trained in the security aspects of their assigned jobs. Initial and ongoing training is a cost of successfully incorporating security measures into support and operations activities.

Another cost is that associated with creating and updating documentation to ensure that security concerns are appropriately reflected in support and operations policies, procedures, and duties.

9 Cryptography

Cryptography is a branch of mathematics based on the transformation of data. It is an important tool for protecting information and is used in many aspects of information security. For example, cryptography can help provide data confidentiality, integrity, electronic signatures, and advanced user authentication. Although modern cryptography relies upon advanced mathematics, users can reap its benefits without understanding its mathematical underpinnings.

NIST has published an array of Special Publications (SPs) and Federal Information Processing Standards (FIPS) that are applicable to the use of cryptography within the Federal Government. A list of such SPs and FIPS can be found in Appendix A of NIST SP 800-175B, *Guideline for Using Crypto Standards: Cryptographic Mechanisms*. Public Laws, Presidential Executive Orders and Directives, and other guidance from organizations in the Executive Office of the President drive the SPs and FIPS written by NIST. Legislative mandates, policies, and directives specific to cryptography are introduced in NIST SP 800-175A, *Guideline for Using Crypto Standards: Directives, Mandates, and Policies*.

Cryptography alone will not satisfy the information assurance needs of any organization. Rather, when combined with other security measures, cryptography is a useful tool for satisfying a wide spectrum of information security needs and requirements. This chapter describes fundamental aspects of the basic cryptographic technologies and some specific ways cryptography can be applied to improve security. The chapter also explores some of the important issues to be considered when incorporating cryptography into systems.

9.1 Uses of Cryptography

Cryptography is used to protect data both inside and outside the boundaries of a system. Data within a system may be sufficiently protected with logical and physical access controls (perhaps supplemented by cryptography). However, outside of the system, cryptography is sometimes the only way to protect data. For instance, data cannot be protected by the originator's logical or physical access controls when in transit across communications lines or resident on another system. Cryptography provides a solution by protecting data even when the data is no longer in the control of the originator.

9.1.1 Data Encryption

One of the best ways to obtain cost-effective data confidentiality is through the use of encryption. Encryption transforms intelligible data, called plaintext, into an unintelligible form, called cipher text. This is reversed through the process of decryption. Once data is encrypted, the cipher text does not have to be protected against disclosure. However, if cipher text is modified, it will not decrypt correctly.

Both secret and public key cryptography can be used for data encryption although not all public key algorithms provide for data encryption. To use a secret key algorithm, data is encrypted using a specific key. The same key must be used to decrypt the data. When public key cryptography is used for encryption, any party may use any other party's public key to encrypt a message. However, only the party with the corresponding private key can decrypt, and thus read, the message. There are several reason to choose one form of cryptography over the other. For example, an organization may decide to go with public key cryptography because it is more secure and convenient to use since private keys do not have to be transmitted to anyone. In order for secret-key cryptography to function, the secret keys must be transmitted due to the fact that the same key is used for the encryption and decryption of that specific data. More detailed guidance on public key infrastructure (PKI) is available in NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, NIST SP 800-57 Part 3, *Recommendation for Key Management: Part 3 – Application Specific Key Management Guidance*, NIST SP 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS).*

9.1.2 Integrity

Integrity is a property whereby data has not been altered in an unauthorized manner since it was created, transmitted, or stored. In systems, it is not always possible for humans to scan information to determine if data has been erased, added, or modified. Even if scanning were possible, the individual may have no way of knowing what the correct data is supposed to be. For example, "do" may be changed to "do not," or $1,000 may be changed to $10,000. It is therefore desirable to have an automated means of detecting both intentional and unintentional modifications of data.

While error detection codes have long been used in communications protocols (e.g., parity bits), these are more effective in detecting and correcting unintentional modifications. Cryptography can effectively detect both intentional and unintentional modification. However, error detection codes, such as parity bits, do not protect files from being modified.

9.1.3 Electronic Signatures

Today's systems store and process documents in electronic form. Having documents in electronic form permits rapid processing and transmission and improves overall efficiency. The approval of a paper document has traditionally been indicated by a written signature. What is needed, therefore, is the electronic equivalent of a written signature that can be recognized as having the same legal status as a written signature. In addition, to the integrity protections discussed above, cryptography can provide a means of linking a document with a particular person, as is done with a written signature. Electronic signatures can use either secret key or public key cryptography. However, public key methods are generally easier to use.

Simply taking a digital picture of a written signature does not provide adequate security. Such a digitized written signature could easily be copied from one electronic document to another with no way to determine whether it is legitimate. Electronic signatures, on the other hand, are unique to the message being signed and will not verify if they are copied to another document.

9.1.3.1 Secret Key Electronic Signatures

An electronic signature can be implemented using secret key message authentication codes, or MACs. For example, if two parties share a secret key, and one party receives data with a MAC that is correctly verified using the shared key, that party may assume that the other party signed the data. This also assumes that the two parties trust each other. Through the use of a MAC, data integrity and a form of electronic signature are obtained. Using additional controls, such as key notarization[6] and key attributes[7], it is possible to provide an electronic signature even if the two parties do not trust each other.

9.1.3.2 Public Key Electronic Signatures

Another type of electronic signature is called a digital signature and is implemented using public key cryptography. Data is electronically signed by applying the originator's private key to the data. (The exact mathematical process for doing this is not important for this discussion.) To increase the speed of the process, the private key is applied to a shorter form of the data, called a "hash" or "message digest," rather than to the entire set of data. The resulting digital signature can be stored or transmitted along with the data. The signature can be verified by any party using the public key of the signer. This feature is very useful, for example, when distributing signed copies of virus-free software. Any recipient can verify that the program remains virus-free. If the signature verifies properly, then the verifier has confidence that the data was not modified after being signed and that the owner of the public key was the signer.

NIST has published standards for a digital signature and a secure hash for use by the federal government in FIPS 186-4, *Digital Signature Standard* and FIPS 180-4, *Secure Hash Standard*.

9.1.4 User Authentication

Authentication is a process that provides assurance of the source of information to a receiving entity. Cryptography can increase security in user authentication techniques. As discussed in section 10.7, cryptography is the basis for several advanced authentication methods. Instead of communicating passwords over an open network, authentication can be performed by demonstrating knowledge of a cryptographic key. Using these methods, a one-time password, which is not susceptible to eavesdropping, can be used. User authentication can use either secret or public key cryptography.

9.2 Implementation Issues

This section explores several important issues to consider when using (e.g., designing, implementing, integrating) cryptography in a system. NIST has developed several FIPS and SPs that apply to the implementation of cryptography in federal information and federal systems. A list of these FIPS and SPs is located in Appendix A of NIST SP 800-175B.

9.2.1 Selecting Design and Implementation Standards

NIST and other organizations have developed numerous standards for designing, implementing, and using cryptography and for integrating it into automated systems. By using these standards,

[6] Key Notarization – is a method, in conjunction with cryptographic facilities (called Key Notarization Facilities), that applies additional security to keys by identifying the sender and recipient, thus, providing assurance on the authenticity of the exchanged keys.

[7] Key Attributes – is a distinct identifier of an entity.

organizations can reduce costs and protect their investments in technology. Standards provide solutions that have been accepted by a wide community and reviewed by experts in relevant areas. Standards help ensure interoperability among different vendors' equipment, thus allowing an organization to select from various products in order to find cost-effective equipment.

Managers and users of systems choose the appropriate cryptographic standard based on a cost-effectiveness analysis, trends in the standard's acceptance, and interoperability requirements. In addition, each standard is carefully analyzed to determine if it is applicable to the organization and the desired application.

9.2.2 Deciding between Hardware, Software, or Firmware Implementations

The trade-offs among security, cost, simplicity, efficiency, and ease of implementation need to be studied by managers acquiring various security products meeting a standard. Cryptography can be implemented in hardware, software, or firmware. Each has its related costs and benefits.

In general, software is less expensive and slower than hardware, although for large applications, hardware may be less expensive. In addition, software may be less secure, since it is more easily modified or bypassed than equivalent hardware products. Tamper resistance in hardware is usually considered more reliable.

In many cases, cryptography is implemented in a hardware device (e.g., electronic chip, ROM-protected processor) but is controlled by software. This software requires integrity protection to ensure that the hardware device is provided with correct information (e.g., controls, data) and is not bypassed. Thus, a hybrid solution is generally provided, even when the basic cryptography is implemented in hardware. Effective security requires correct management of the entire hybrid solution.

Firmware can be found in nearly every piece of technology used today, including cell phones, smart TVs, and even in USB keyboards. Thus, securing firmware implementations is critical. One way to protect your system is by purchasing hardware with built-in protection that prevents malicious firmware modification. For more information on hardening firmware, refer to NIST SP 800-147, *BIOS Protection Guidelines*, and NIST SP 800-155 (DRAFT), *BIOS Integrity Measurement Guidelines*.

9.2.3 Managing Keys

The security of information protected by cryptography directly depends upon the protection afforded to keys. All keys need to be protected against modification, and secret and private keys require protection against unauthorized disclosure. Key management involves the procedures and protocols, both manual and automated, used throughout the entire life cycle of the keys. This includes the generation, distribution, storage, entry, use, destruction, and archiving of cryptographic keys.

In a small community of users, public keys and their "owners" can be strongly bound by simply exchanging public keys (e.g., putting them on a CD-ROM or other media). However, conducting electronic business on a larger scale—potentially involving geographically and organizationally distributed users—necessitates a means for obtaining public keys electronically with a high degree of confidence in their integrity and binding to individuals. The support for the binding between a key and its owner is generally referred to as a public key infrastructure.

Users also need the ability to enter the community of key holders, generate keys (or have them generated on their behalf), disseminate public keys, revoke keys (for example, in case of compromise of the private key), and change keys. In addition, it may be necessary to incorporate time/date stamping and to archive keys for verification of old signatures.

For more information on key management, see NIST SP 800-57 Part 1, *Recommendation for Key Management, part 1: General,* NIST SP 800-57 Part 2, *Recommendation for Key Management,* Part 2*: Best Practices for Key Management Organization,* and NIST SP 800-57 Part 3, *Recommendation for Key Management, part 3: Application-Specific Key Management Guidance.*

9.2.4 Security of Cryptographic Modules

Cryptography is typically implemented in a module of software, firmware, hardware, or some combination thereof. This module contains the cryptographic algorithm(s), certain control parameters, and temporary storage facilities for the key(s) being used by the algorithm(s). The proper functioning of cryptography requires the secure design, implementation, and use of the cryptographic module. This includes protecting the module against tampering.

Conformance to standards can be important for many reasons, including interoperability or strength of security provided. NIST established the Cryptographic Module Validation Program (CMVP) which validates cryptographic modules to Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*. The goal of the CMVP is to promote the use of validated cryptographic modules and provide federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules. A list of modules that have been validated by NIST is available on the Computer Security Resource Center (CSRC) website.

FIPS 140-2 specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The standard defines four security levels for cryptographic modules, with each level providing a significant increase in security over the preceding level. The four levels allow for cost-effective solutions that are appropriate for varying degrees of data sensitivity and different application environments. The user can select the best module for any given application or system, avoiding the cost of unnecessary security features.

9.2.5 Applying Cryptography to Networks

The use of cryptography within networking applications often requires special considerations. In these applications, the suitability of a cryptographic module may depend on its capability for handling special requirements imposed by locally attached communications equipment or by the network protocols and software.

Encrypted information, MACs, or digital signatures may require transparent communications protocols or equipment to avoid being misinterpreted by the communications equipment or software as control information. It may be necessary to format the encrypted information, MAC, or digital signature to ensure that it does not confuse the communications equipment or software. It is essential that cryptography satisfy the requirements imposed by the communications equipment and does not interfere with the proper and efficient operation of the network.

Data is encrypted on a network using either link encryption or end-to-end encryption. In general, link encryption is performed by service providers, such as a data communications provider. Link encryption encrypts all of the data along a communications path (e.g., a satellite link, telephone circuit, T3 line). Since link encryption also encrypts routing data, communications nodes need to decrypt the data to continue routing. In end-to-end encryption, data is encrypted when being passed through a network, but routing information remains visible. End-to-end encryption is generally performed by the end user organization. Some examples of modern usage of end-to-end encryption include Pretty Good Privacy (PGP) and Secure/Multipurpose Internal Mail Extensions (S/MIME) for email. It is possible to combine both types of encryption.

9.2.6 Complying with Export Rules

The U.S. Government controls the export of cryptographic implementations. The rules governing export can be quite complex since they consider multiple factors. Additionally, cryptography is a rapidly evolving field, and rules may change from time to time. Address questions concerning the export of a particular implementation to the appropriate legal counsel.

9.3 Interdependencies

There are many interdependencies among cryptography and other security controls highlighted in this publication. Cryptography both depends on other security safeguards and assists in providing them. For example,

- *Physical Security*. Physical protection of a cryptographic module is required to prevent—or at least detect—physical replacement or modification of the cryptographic system and the keys within it. In many environments (e.g., open offices, laptops), the cryptographic module itself has to provide the desired levels of physical security. In other environments (e.g., closed communications facilities, steel-encased Cash-Issuing Terminals), a cryptographic module may be safely employed within a secured facility.
- *User Authentication*. Cryptography can be used both to protect passwords that are stored in systems and to protect passwords that are communicated between systems. Furthermore, cryptographic-based authentication techniques may be used in conjunction with or in place of password-based techniques to provide stronger authentication of users.
- *Logical Access Control*. In many cases, cryptographic software may be embedded within a host system, and it may not be feasible to provide extensive physical protection to the host system. In these cases, logical access control may provide a means of isolating the cryptographic software from other parts of the host system, protect the cryptographic software from tampering, and safeguard the keys from replacement or disclosure. The use of such controls provides the equivalent of physical protection.
- *Audit Trails*. Cryptography may play a useful role in audit trails, which are used to help support electronic signatures. Audit records may require signatures, and cryptography

may be needed to protect audit records stored on systems from disclosure or modification.

- *Assurance*. Assurance that a cryptographic module is properly and securely implemented is essential to the effective use of cryptography. NIST maintains validation programs for several of its standards for cryptography (see section 9.2.4). Vendors can have their products validated for conformance to the standard through a rigorous set of tests. Such testing provides increased assurance that a module meets stated standards, and system designers, integrators, and users can have greater confidence that validated products conform to accepted standards.

Cryptographic systems are monitored and periodically audited to ensure that they are still satisfying their security objectives. All parameters associated with correct operation of the cryptographic system are reviewed; operation of the system itself is periodically tested; and the results are audited. Certain information, such as secret keys or private keys in public key systems, are not subject to audit. However, non-secret or non-private keys could be used in a simulated audit procedure.

9.4 Cost Considerations

Using cryptography to protect information has both direct and indirect costs, which are determined in part by product availability. A wide variety of products exist for implementing cryptography in integrated circuits, add-on boards or adapters, and stand-alone units.

9.4.1 Direct Costs

The direct costs of cryptography include:

- Acquiring or implementing the cryptographic module and integrating it into the system. The medium (i.e., hardware, software, firmware, or a combination thereof) and various other issues such as level of security, logical and physical configuration, and special processing requirements will have an impact on cost.
- Managing the cryptography and the cryptographic keys generation, distribution, archiving, and disposition as well as security measures to protect the keys.

9.4.2 Indirect Costs

The indirect costs of cryptography include:

- A decrease in system or network performance, resulting from the additional overhead of applying cryptographic protection to stored or communicated data.
- Changes in the way users interact with the system, resulting from more stringent security enforcement. However, cryptography can be made nearly transparent to the users so that the impact is minimal.

10 Control Families

To ensure the protection of confidentiality, integrity, and availability, FIPS 200 specifies minimum security requirements in seventeen security-related areas. The areas, which are introduced below, represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting federal information and systems.

The intent of this section is to provide a brief description of each security control family. Each family has a list of controls that address a specific security goal. To view the complete security control catalog and a description of all controls, refer to NIST SP 800-53.

10.1 Access Control (AC)

On many multiuser systems, requirements for using—and prohibitions against the use of—various system resources vary considerably. For example, some information must be accessible to all users, some may be needed by several groups or departments, and some may be accessed by only a few individuals. While users must have access to specific information needed to perform their jobs, denial of access to non-job-related information may be required. It may also be important to control the kind of access that is permitted (e.g., the ability for the average user to execute, but not change, system programs). These types of access restrictions enforce policy and help ensure that unauthorized actions are not taken.

Access is the ability to make use of any system resource. Access control is the process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances). System-based access controls are called logical access controls. Logical access controls can prescribe not only who or what (in the case of a process) is to have access to a specific system resource but also the type of access that is permitted. These controls may be built into the operating system, incorporated into applications programs or major utilities (e.g., database management systems, communications systems), or implemented through add-on security packages. Logical access controls may be implemented internally to the system being protected or in external devices.

Examples of access control security controls include: account management, separation of duties, least privilege, session lock, information flow enforcement, and session termination.

Organizations limit: (i) system access to authorized users; (ii) processes acting on behalf of authorized users; (iii) devices, including other systems; and (iv) the types of transactions and functions that authorized users are permitted to exercise.

10.2 Awareness and Training (AT)

Often, it is the user community that is recognized as being the weakest link in securing systems. Making system users aware of their security responsibilities and teaching them correct practices helps change their behavior. It also supports individual accountability, which is one of the most important ways to improve information security. Without knowing the necessary security measures or to how to use them, users cannot be truly accountable for their actions. The importance of this training is emphasized in the Computer Security Act, which requires training for those involved with the management, use, and operation of federal systems.

The purpose of information security awareness, training, and education is to enhance security by (i) raising awareness of the need to protect system resources; (ii) developing skills and knowledge so system users can perform their jobs more securely; and (iii) building in-depth knowledge as needed to design, implement, or operate security programs for organizations and systems. The organization is responsible for making sure that managers and users are aware of the security risks associated with their activities and that organizational personnel are adequately trained to carry out their information security-related duties and responsibilities.

Examples of awareness and training security controls include: security awareness training, role-based security training, and security training records.

Organizations: (i) ensure that managers and users of organizational systems are made aware of the security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

10.3 Audit and Accountability (AU)

An audit is an independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures. An audit trail is a record of individuals who have accessed a system as well as what operations the user has performed during a given period. Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance issues, and flaws in applications.

Audit trails may be used as a support for regular system operations, a kind of insurance policy, or both. As insurance, audit trails are maintained but not used unless needed (e.g., after a system outage). As a support for operations, audit trails are used to help system administrators ensure that the system or resources have not been harmed by hackers, insiders, or technical problems.

Examples of audit and accountability controls include: audit events, time stamps, non-repudiation, protection of audit information, audit record retention, and session audit.

Organizations: (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity; and (ii) ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable.

10.4 Security Assessment and Authorization (CA)

A security control assessment is the testing and/or evaluation of the management, operational, and technical security controls in a system 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. The assessment also helps determine if the implemented controls are the most effective and cost-efficient solution for the function they are intended to serve. Assessment of the security controls is done on a continuous basis to support a near real-time analysis of the organizations current security posture.

Following a complete and thorough security control assessment, the authorizing official makes the decision to authorize the system to operate or to continue to operate.

Examples of security assessment and authorization controls include: security assessments system interconnections, plans of action and milestones, and continuous monitoring.

Organizations: (i) periodically assess the security controls in organizational systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems; (iii) authorize the operation of organizational systems and any associated system connections; and (iv) monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

10.5 Configuration Management (CM)

Configuration management is a collection of activities focused on establishing and maintaining the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle (CNSSI 4009). Configuration management consists of determining and documenting the appropriate specific settings for a system, conducting security impact analyses, and managing changes through a change control board. It allows the entire system to be reviewed to help ensure that a change made on one system does not have adverse effects on another system. For more information on configuration management, see NIST SP 800-128.

Checklists can also be used to verify that changes to the system have been reviewed from a security point-of-view. A common audit examines the system's configuration to see if major changes (such as connecting to the Internet) have occurred that have not yet been analyzed. The NIST checklist repository, maintained as part of the National Vulnerability Database (NVD), provides multiple checklists which can be used to check compliance with the secure configuration specified in the system security plan. The checklists can be accessed at https://web.nvd.nist.gov/view/ncp/repository.

Examples of configuration management controls include: baseline configuration, configuration change control, security impact analysis, least functionality, and software usage restrictions.

Organizations: (i) establish and maintain baseline configurations and inventories of organizational systems, including hardware, software, firmware, and documentation throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational systems.

10.6 Contingency Planning (CP)

An information security contingency is an event with the potential to disrupt system operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, fire, or storm. Particularly destructive events are often referred to as disasters. To avert potential contingencies and disasters or minimize the damage they cause, organizations can take early steps to control the event. Generally, this activity is called contingency planning.

A contingency plan is a management policy and procedure used to guide organizational response to a perceived loss of mission capability. The Information System Contingency Plan (ISCP) is used by risk managers to determine what happened, why, and what to do. The ISCP may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan (DRP) for major disruptions. Contingency planning involves more than planning for a move offsite after a disaster destroys a data center. It also addresses how to keep an organization's critical functions operational in the event of disruptions, both large and small. This broader perspective on contingency planning is based on the distribution of system support throughout an organization. For more information on contingency planning, see NIST SP 800-34.

Examples of contingency planning controls include: contingency plan, contingency training, contingency plan testing, system backup, and system recovery and restitution.

Organizations: (i) establish, maintain, and effectively implement plans for emergency response, (ii) backup operations, and (iii) oversee post-disaster recovery for organizational systems to ensure the availability of critical information resources and the continuity of operations in emergency situations.

10.7 Identification and Authentication (IA)

Identification is the means of verifying the identity of a user, process, or device, typically as a prerequisite for granting access to resources in an IT system.

For most systems, identification and authentication is the first line of defense. Identification and authentication is a technical measure that prevents unauthorized individuals or processes from entering a system.

Identification and authentication is a critical building block of information security since it is the basis for most types of access control and for establishing user accountability. Access control often requires that the system be able to identify and differentiate between users. For example, access control is often based on least privilege, which refers to granting users only those accesses required to perform their duties. User accountability requires linking activities on a system to specific individuals and, therefore, requires the system to identify users.

Systems recognize individuals based on the authentication data the systems receive. Authentication presents several challenges: collecting authentication data, transmitting the data securely, and knowing whether the individual who was originally authenticated is still the individual using the system. For example, a user may walk away from a terminal while still logged on, and another person may start using it.

There are four means of authenticating a user's identity that can be used alone or in combination. User identity can be authenticated based on:

- something the individual knows – e.g., a password, Personal Identification Number (PIN), or cryptographic key
- something the individual possesses (a token) – e.g., an ATM card or a smart card
- something the individual is (static biometric) – e.g., fingerprint, retina, face
- something the individual does (dynamic biometrics) – e.g., voice pattern, handwriting, typing rhythm

While it may appear that any of these individual methods could provide strong authentication, there are problems associated with each. If an individual wanted to impersonate someone else on a system, they can guess or learn another user's password or steal or fabricate tokens. Each method also has drawbacks for legitimate users and system administrators: users forget passwords and may lose tokens, and administrative overhead for keeping track of identification and authorization data and tokens can be substantial. Biometric systems have significant technical, user acceptance, and cost problems as well.

Examples of identification and authentication controls include: device identification and authentication, identifier management, authenticator management, authenticator feedback, and re-authentication.

Organizations: (i) identify system users, processes acting on behalf of users, or devices and (ii) authenticate or verify the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.

10.8 Incident Response (IR)

Systems are subject to a wide range of threat events, from corrupted data files to viruses to natural disasters. Vulnerability to some threat events can be mitigated by standard operating procedures. For example, frequently occurring events like mistakenly deleting a file can usually be repaired through restoration from the backup file. More severe threat events, such as outages caused by natural disasters, are normally addressed in an organization's contingency plan. Other damaging events result from deliberate malicious technical activity (e.g., the creation of viruses, system hacking).

Threat events can result from a virus, other malicious code, or a system intruder (either an insider or an outsider). They can more generally refer to those incidents that could result in severe damage without a technical expert response. An example of a threat event that would require an immediate technical response would be an organization experiencing a denial-of-service attack. This kind of attack would require swift action on the part of the incident response team in order to reduce the affect the attack will have on the organization. The definition of a threat event is somewhat flexible and may vary by organization and computing environment.

Although the threats that hackers and malicious code pose to systems and networks are well known, the occurrence of such harmful events remains unpredictable. Security incidents on larger networks (e.g., the Internet), such as break-ins and service disruptions, have harmed various organizations' computing capabilities. When initially confronted with such incidents, most organizations respond in an ad hoc manner. However, recurrence of similar incidents can make it cost-beneficial to develop a standing capability for quick discovery of and response to such events. This is especially true since incidents can often "spread" when left unchecked, thus escalating the damage and seriously harming an organization.

Incident handling is closely related to contingency planning. An incident handling capability may be viewed as a component of contingency planning because it allows for the ability to react quickly and efficiently to disruptions in normal processing. Broadly speaking, contingency planning addresses events with the potential to interrupt system operations. Incident handling can be considered that portion of contingency planning specifically that responds to malicious technical threats. For more information on incident response, see NIST SP 800-61, *Computer Security Incident Handling Guide.*

Examples of incident response controls include: incident response training, incident response testing, incident handling, incident monitoring, and incident reporting.

Organizations: (i) establish an operational incident handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

10.9 Maintenance (MA)

To keep systems in good working order and to minimize risks from hardware and software, it is paramount that organizations establish procedures for the maintenance of organizational systems. There are many different ways an organization can address these maintenance requirements.

Controlled maintenance of a system deals with maintenance that is scheduled and performed in accordance the with manufacturer's specifications. Maintenance performed outside of a scheduled cycle, known as corrective maintenance, occurs when a system fails or generates an error condition that must be corrected in order to return the system to operational conditions. Maintenance can be performed locally or non-locally. Nonlocal maintenance is any maintenance or diagnostics performed by individuals communicating through a network either internally or externally (e.g. the Internet).

Examples of maintenance controls include: controlled maintenance, maintenance tools, nonlocal maintenance, maintenance personnel, and timely maintenance.

Organizations: (i) perform periodic and timely maintenance on organizational systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

10.10 Media Protection (MP)

Media protection is a control that addresses the defense of system media, which can be described as both digital and non-digital. Examples of digital media include: diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks.

Examples of non-digital media include paper or microfilm.

Media protections are put in place to address several issues with regard to digital and non-digital media. These protections can restrict access and make certain file types available to authorized personnel only, apply security labels to sensitive information, and provide instructions on how to remove information from media such that the information cannot be retrieved or reconstructed. Media protections also include physically controlling system media and ensuring accountability as well as restricting mobile devices capable of storing information and carrying it outside of restricted areas.

Examples of media protection controls include: media access, media marking, media storage, media transport, and media sanitization.

Organizations: (i) protect system media, both paper and digital; (ii) limit access to information on system media to authorized users; and (iii) sanitize or destroy system media before disposal or release for reuse.

10.11 Physical and Environmental Security (PE)

The term physical and environmental security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. Physical and environmental controls cover three broad areas:

1. The physical facility is typically the building, other structure, or vehicle housing the system and network components. Systems can be characterized, based upon their operating location, as static, mobile, or portable. Static systems are installed in structures at fixed locations. Mobile systems are installed in vehicles that perform the function of a structure, but not at a fixed location. Portable systems may be operated in a wide variety of locations, including buildings, vehicles, or in the open. The physical characteristics of these structures and vehicles determine the level of physical threats such as fire, roof leaks, or unauthorized access.

2. The facility's general geographic operating location determines the characteristics of natural threats, which include earthquakes and flooding; man-made threats such as burglary, civil disorders, or interception of transmissions and emanations; and damaging nearby activities, including toxic chemical spills, explosions, fires, and electromagnetic interference from emitters (e.g., radars).

3. Supporting facilities are those services (both technical and human) that maintain the operation of the system. The system's operation usually depends on supporting facilities such as electric power, heating and air conditioning, and telecommunications. The failure or substandard performance of these facilities may interrupt operation of the system and cause physical damage to system hardware or stored data.

Examples of physical and environmental controls include: physical access authorizations, physical access control, monitoring physical access, emergency shutoff, emergency power, emergency lighting, alternate work site, information leakage, and asset monitoring and tracking.

Organizations: (i) limit physical access to systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for systems; (iii) provide supporting utilities for systems; (iv) protect systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing systems.

10.12 Planning (PL)

Systems have increasingly taken on a strategic role in the organization. They assist organizations in conducting their daily activities and support decision making. With proper planning, systems can provide a security level commensurate with the risk associated with the operation of the system, improve productivity and performance, and enable new ways of managing and organizing. Planning for systems is crucial in the development and implementation of the organization’s information security goals.

System security plans are developed to provide an overview of the security requirements of the system and how the security controls and control enhancements meet those security requirements. Having security controls in place does not guarantee the overall protection of a system. Users, by far, have proven to be the weakest link in the security of organizational systems. With one intentional or unintentional errant click, the security posture of an entire system can be compromised. To combat this, it is incumbent on the organization to assign rules based on individual roles and responsibilities.

Examples of planning controls include: system security plan, rules of behavior, security concept of operations, information security architecture, and central management.

Organizations: develop, document, periodically update, and implement security plans for organizational systems that describe the security controls in place or planned for the system as well as the rules of behavior for individuals accessing the systems.

10.13 Personnel Security (PS)

Many important issues in information security involve users, designers, implementers, and managers. A broad range of security issues relate to how these individuals interact with system components as well as the access and authorities needed to do their jobs. No system can be secured without properly addressing these security issues.

Personnel security seeks to minimize the risk that staff (permanent, temporary, or contractor) pose to organizational assets through the malicious use or exploitation of their legitimate access to the organization’s resources. An organization’s status and reputation can be adversely affected by the actions of its employees. Employees may have access to extremely sensitive, confidential, or proprietary information, the disclosure of which can destroy an organizations reputation or cripple it financially. Therefore, organizations must be vigilant when recruiting and hiring new employees, as well as when an employee transfers or is terminated. The sensitive nature and value of organizational assets requires in-depth personnel security measures.

Examples of personnel control include: personnel screening, personnel termination, personnel transfer, access agreements, and personnel sanctions.

Organizations: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

10.14 Risk Assessment (RA)

Organizations are dependent upon information technology and associated systems to successfully carry out their missions. The increasing amount of information technology products used in various organizations and industries can be beneficial, may also introduce serious threats that can adversely affect an organization's operations and assets, individuals, other organizations, and the Nation by exploiting both known and unknown vulnerabilities. The exploitation of vulnerabilities in organizational systems can compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems.

Performing a risk assessment is a fundamental component of risk management as described in NIST SP 800-39. Risk assessments identify and prioritize risks to organizational operations, assets, individuals, other organizations, and the Nation that may result from the operation of a system. Risk assessments, which can be conducted at all three tiers in the risk management hierarchy, inform decision makers and support risk responses by identifying: (i) relevant threats to organizations or threats directed through organizations against other organizations; (ii) vulnerabilities both internal and external to organizations; (iii) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur. For more information on risk assessments, see NIST SP 800-30.

Examples of risk assessment controls include: security categorization, risk assessment, vulnerability scanning, and technical surveillance countermeasures survey.

Organizations: periodically assess the risk to organizational operations (e.g., mission, functions, image, reputation), organizational assets, and individuals, which may result from the operation of organizational systems and the associated processing, storage, or transmission of organizational information.

10.15 System and Services Acquisition (SA)

Like other aspects of information processing systems, security is most effective and efficient if planned and managed throughout a system's life cycle, from initial planning to design, implementation, operation, and disposal. Many security-relevant events and analyses occur during a system's life. It is equally important that developers include individuals on the development team who possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the system. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes.

SSPs can be developed for a system at any point in the life cycle. However, to minimize costs and prevent the disruption of ongoing operations, the recommended approach is to incorporate the plan at the beginning of the systems life cycle. It is significantly more expensive to add security features to a system than it is to include them from the very beginning. Security, once added, is not a function which does not require frequent updating/upgrading. It is important to ensure security requirements keep pace with changes to the computing environment, technology, and personnel. While some systems might find it useful to constantly update their SSP, other systems may only require updates after each phase of the systems life cycle or after each re-accreditation.

Examples of system and service acquisition controls include: allocation of resources, acquisition process, system documentation, supply chain protection, trustworthiness, criticality analysis, developer-provided training, component authenticity, and developer screening.

Organizations: (i) allocate sufficient resources to adequately protect organizational systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

10.16 System and Communication Protection (SC)

System and communications protection controls provide an array of safeguards. Some of the controls in this family address the confidentiality and integrity of information at rest and in transit. The protection of confidentiality and integrity can be provided by these controls through physical or logical means. For example, an organization can provide physical protection by segregating certain functions to separate servers, each having its own set of IP addresses.

Organizations can better safeguard their information by separating user functionality and system management functionality. Providing this type of protection prevents the presentation of system management-related functionality on an interface for non-privileged users. System and communications protection also establishes boundaries that restrict access to publicly accessible information within a system. Using boundary protections, an organization can monitor and control communications at external boundaries as well as key internal boundaries within the system.

Examples of system and communication protection controls include: application partitioning, denial of service protection, boundary protection, trusted path, mobile code, session authenticity, thin nodes, honeypots, transmission confidentiality and integrity, operations security, protection of information at rest and in transit, and usage restrictions.

Organizations: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of the systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

10.17 System and Information Integrity (SI)

Integrity is defined as guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. It is the assertion that data can only be accessed or modified by the authorized personnel. System and information integrity provides assurance that the information being accessed has not been meddled with or damaged by an error in the system.

Examples of system and information integrity controls include: flaw remediation, malicious code protection, security function verification, information input validation, error handling, non-persistence, and memory protection.

Organizations: (i) identify, report, and correct information and system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational systems; and (iii) monitor system security alerts and advisories and respond appropriately.

10.18 Program Management (PM)

Systems and the information they process are critical to many organizations' ability to perform their missions and business functions. It therefore makes sense that executives view system security as a management issue and seek to protect their organization's information technology resources as they would any other valuable asset. To do this effectively requires the development of a comprehensive management approach.

Many security programs, distributed throughout the organization, have different elements performing various functions. While this approach has benefits, the distribution of the system security functions in many organizations is haphazard, usually based upon history (i.e., who was available in the organization to do what when the need arose). Ideally, the distribution of system security functions is the result of a planned and integrated management philosophy.

Managing system security at multiple levels produces numerous benefits. Each level contributes to the overall system security program with different types of expertise, authority, and resources. In general, higher-level officials (e.g., those at the headquarters, unit levels in the agency described above) better understand the organization as a whole and have more authority. On the other hand, lower-level officials (e.g., at the system facility and applications levels) are more familiar with the specific technical and procedural requirements and problems of the systems and users. The levels of system security program management are complementary; each can help the other be more effective.

Examples of project management controls include: information security program plan, information security resources, plan of action and milestone process, system inventory, enterprise architecture, risk management strategy, insider threat program, and threat awareness program.

Appendix A—References

[CSA of 1987] Computer Security Act of 1987, Public Law 100-235, 101 Stat 1724 https://www.gpo.gov/fdsys/pkg/STATUTE-101/pdf/STATUTE-101-Pg1724.pdf

[E-Gov Act] E-Government Act of 2002, Pub. L. 107-347, 116 Stat 2899. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[Clinger-Cohen Act] Clinger-Cohen Act, Public Law 107-217, 116 Stat 1234. https://www.gpo.gov/fdsys/pkg/USCODE-2011-title40/pdf/USCODE-2011-title40-subtitleIII.pdf

[FISMA2002] Federal Information Security Management Act of 2002, Pub. L. 107-347 (Title III), 116 Stat. 2946. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[FISMA2014] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. http://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf.

[OMB Circular A-130] Office of Management and Budget (OMB), *Management of Federal Information Resources*, OMB Memorandum Circular A-130, Revised July 28, 2016. https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf [accessed 8/15/16].

[OMB Memo 04-04] Office of Management and Budget (OMB), *E-Authentication Guidance for Federal Agencies*, OMB Memorandum 04-04, December 16, 2003. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf [accessed 7/27/16].

[OMB Memo 06-15] Office of Management and Budget (OMB), *Safeguarding Personally Identifiable Information*, OMB Memorandum 06-15, May 22, 2006. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m-06-15.pdf [accessed 7/27/16].

[OMB Memo 06-16] Office of Management and Budget (OMB), *Protection of Sensitive Agency Information*, OMB Memorandum 06-16, June 23, 2006. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf [accessed 7/27/16].

[OMB Memo 06-19] Office of Management and Budget (OMB), *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, OMB Memorandum 06-19, July 12, 2006. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m-

06-19.pdf [accessed 7/27/16].

[OMB Memo 14-03] Office of Management and Budget (OMB), *Enhancing the Security of Federal Information and Information Systems*, OMB Memorandum 14-03, November 18, 2013. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf [accessed 7/27/16].

[FIPS140-2] U.S. Department of Commerce. *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards (FIPS) Publication 140-2, May 2001 (change notice December 2002), 69pp. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf [accessed 7/26/16].

[FIPS180-4] U.S. Department of Commerce. *Secure Hash Standard (SHS)*, Federal Information Processing Standards (FIPS) Publication 180-4, August 2015, 36pp. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf [accessed 7/26/16].

[FIPS186-4] U.S. Department of Commerce. *Digital Signature Standard (DSS)*, Federal Information Processing Standards (FIPS) Publication 186-4, July 2013, 130pp. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf [accessed 7/26/16].

[FIPS199] U.S. Department of Commerce. *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 199, February 2004, 13pp. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [accessed 7/26/16].

[FIPS200] U.S. Department of Commerce. *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 200, March 2006, 17pp. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf [accessed 7/26/16].

[NISTIR 7298] Kissel, R., *Glossary of Key Information Security Terms*, NISTIR 7298 Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2013, 222pp. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[NISTIR 8062] Brooks, S., Garcia, M., Lefkovitz, N., Lightman, S., Nadeau, E., An Introduction to Privacy Engineering and Risk Management in Federal Systems, NISTIR 8062, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2017, 49pp.

http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

[SP800-18] NIST Special Publication (SP) 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2006, 48pp.

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf

[SP800-30] NIST Special Publication (SP) 800-30 Revision 1, *Guide for Conducting Risk Assessments*, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, 95pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[SP800-32] NIST Special Publication (SP) 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2001, 54pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[SP800-34] NIST Special Publication (SP) 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2010 (updated November 2010), 149pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[SP800-37] NIST Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2010 (updated June 2014), 102pp. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

[SP800-39] NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2011, 88pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

[SP800-53] NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013 (updated January 2015), 462pp. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[SP800-53A] NIST Special Publication (SP) 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2014, 487pp.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

[SP800-57 part 1] NIST Special Publication (SP) 800-57 part 1 Revision 4, *Recommendation for Key Management, Part 1: General*, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2016, 160pp. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

[SP800-57 part 2] NIST Special Publication (SP) 800-57 part 2, *Recommendation for Key Management, Part 2: Best Practices for Key Management Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2005, 79pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p2.pdf

[SP800-57 part 3] NIST Special Publication (SP) 800-57 part 3 Revision 1, *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2015, 102pp. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf

[SP800-60] NIST Special Publication (SP) 800-60 volume 1 Revision 1, *Guide for Mapping Types of Information Systems to Security Categories*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2008, 53pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

[SP800-61] NIST Special Publication (SP) 800-61 Revision 2, *Computer Security Incident Handling Guide*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2012, 79pp. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[SP800-82] NIST Special Publication (SP) 200-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2015, 247pp. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[SP800-95] NIST Special Publication (SP) 800-95, *Guide to Secure Web Services*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2007, 128pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf

[SP800-128] NIST Special Publication (SP) 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2011, 88pp.

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-128.pdf

[SP800-137] NIST Special Publication (SP) 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2011, 80pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

[SP800-147] NIST Special Publication (SP) 800-147, *BIOS Protection Guidelines*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2011, 26pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf

[SP800-152] NIST Special Publication (SP) 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)*, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2015, 147pp. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-152.pdf

[SP800-155] NIST Special Publication (SP) 800-155 (DRAFT), *BIOS Integrity Measurement Guidelines*, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2011, 47pp. http://csrc.nist.gov/publications/drafts/800-155/draft-SP800-155_Dec2011.pdf

[SP800-160] NIST Special Publication (SP) 800-160 (DRAFT), *Systems Security Engineering Guideline: An Integrated Approach to Building Trustworthy Resilient Systems*, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2016, 307pp. http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf

[SP800-161] NIST Special Publication (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2015, 282pp. http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

[SP800-175A] NIST Special Publication (SP) 800-175A (DRAFT), *Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2016, 32pp. http://csrc.nist.gov/publications/drafts/800-175/sp800-175a_draft.pdf

[SP800- NIST Special Publication (SP) 800-175B (DRAFT), *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic*

175B] *Mechanisms*, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2016, 77pp. http://csrc.nist.gov/publications/drafts/800-175/sp800-175b_draft.pdf

Appendix B—**Glossary**

Access Control	The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances). SOURCE: FIPS 201-2
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. SOURCE: SP 800-27 Rev. A
Assurance	Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. “Adequately met” includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass. SOURCE: SP 800-27 Rev. A
Attack	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. SOURCE: CNSSI-4009
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. SOURCE: CNSSI-4009
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

	SOURCE: FIPS 200
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges. SOURCE: CNSSI-4009
Authorizing Official (AO)	A senior (federal) official or executive with the authority to formally assume responsibility for operating a system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. SOURCE: SP 800-37 Rev 1
Biometrics	A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics. SOURCE: FIPS 201
Bit	A binary digit having a value of 0 or 1. SOURCE: FIPS 180-4
Challenge-Response Protocol	An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a secret (often by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the verifier. The verifier can independently verify the response generated by the Claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the Claimant possesses and controls the secret. SOURCE: SP 800-63-2
Checksum	A value that (a) is computed by a function that is dependent on the content of a data object and (b) is stored or transmitted together with the object, for detecting changes in the data SOURCE: IETF RFC 4949 Ver. 2
Ciphertext	Data in its encrypted form.

	SOURCE: SP 800-57 Part 1 Rev. 4
Digital Signature	The result of a cryptographic transformation of data which, when properly implemented, provides the services of: 1. origin authentication, 2. data integrity, and 3. signer non-repudiation. SOURCE: FIPS 140-2
Encryption	The cryptographic transformation of data to produce ciphertext. SOURCE: ISO 7498-2
End-to-End Encryption	Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible.
Firewall	A gateway that limits access between networks in accordance with local security policy. SOURCE: SP 800-32
Gateway	An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks. SOURCE: IETF RFC 4949 Ver. 2
Hacker	Unauthorized user who attempts to or gains access to an information system. SOURCE: CNSSI-4009
Information	1. Facts and ideas, which can be represented (encoded) as various forms of data. 2. Knowledge—e.g., data, instructions—in any medium or form that can be communicated between system entities. SOURCE: IETF RFC 4949 Ver. 2
Information Assurance	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially

	impact IA related terms. SOURCE: CNSSI-4009
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. SOURCE: 44 U.S.C., Sec. 3542
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information. SOURCE: CNSSI-4009
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or a system. SOURCE: SP 800-30 Rev 1
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.] SOURCE: 44 U.S.C., Sec. 3502
Information Technology	(A) with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use— (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; (B) includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services

	(including support services), and related resources; but (C) does not include any equipment acquired by a federal contractor incidental to a federal contract. SOURCE: 40 U.S.C., Sec. 11101
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. SOURCE: 44 U.S.C., Sec. 3542
Intrusion Detection System (IDS)	Software that automates the intrusion detection process. SOURCE: SP 800-94
Key	A parameter used in conjunction with a cryptographic algorithm that determines its operation. Examples applicable to this Standard include: 1. The computation of a digital signature from data, and 2. The verification of a digital signature. SOURCE: FIPS 186-4
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors) during the entire lifecycle of the keys, including their generation, storage, establishment, entry and output, use and destruction. SOURCE: SP 800-57 Part 1 Rev 4
Keystroke Monitoring	The process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails.
Least Privilege	The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. SOURCE: CNSSI-4009
Link Encryption	Encryption of information between nodes of a communications system.

	SOURCE: CNSSI-4009
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
	SOURCE: SP 800-53
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
	SOURCE: SP 800-83
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
	SOURCE: FIPS 140-2
Penetration Testing	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system.
	SOURCE: SP 800-53
Private Key	A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.
	SOURCE: FIPS 140-2
Privilege	A right granted to an individual, a program, or a process.
	SOURCE: CNSSI-4009
Public Key	A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public.
	SOURCE: FIPS 140-2
Public Key Cryptography	Encryption system that uses a public-private key pair for encryption and/or digital signature.
	SOURCE: CNSSI-4009

Public Key Infrastructure (PKI)	A Framework that is established to issue, maintain, and revoke public key certificates. SOURCE: FIPS 186-4
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [Note: System-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.] SOURCE: SP 800-37
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. SOURCE: SP 800-39
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. SOURCE: SP 800-39
Risk Management Framework (RMF)	A structured approach used to oversee and manage risk for an enterprise. SOURCE: CNSSI-4009
Role	A job function or employment position to which people or other system entities may be assigned in a system.

	SOURCE: IETF RFC 4949 Ver 2
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for a system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. SOURCE: FIPS 200
Secret Key	A cryptographic key, used with a secret key cryptographic algorithm, that is uniquely associated with one or more entities and should not be made public. SOURCE: FIPS 140-2
Security	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach. SOURCE: CNSSI-4009
Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in a system 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. SOURCE: SP 800-37
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system and its information. SOURCE: FIPS 199
Security Engineering	An interdisciplinary approach and means to enable the realization of secure systems. It focuses on defining customer needs, security protection requirements, and required functionality early in the systems development life cycle, documenting requirements, and then proceeding with design, synthesis, and system validation while

	considering the complete problem.
	SOURCE: CNSSI-4009
Security Label	The means used to associate a set of security attributes with a specific information object as part of the data structure for that object.
	SOURCE: SP 800-53
Sensitivity	A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.
	SOURCE: SP 800-60
Signature	A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.
	SOURCE: SP 800-61
Spam	Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
	SOURCE: CNSSI-4009
Spyware	Software that is secretly or surreptitiously installed into a system to gather information on individuals or organizations without their knowledge; a type of malicious code.
	SOURCE: SP 800-53
System Integrity	The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.
	SOURCE: SP 800-27
System Security Plan	Formal document that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements.
	SOURCE: SP 800-18
Tailoring	The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via

	explicit assignment and selection statements. SOURCE: SP 800-37
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 a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. SOURCE: SP 800-30
Token	Something that the Claimant possesses and controls (typically a key or password) that is used to authenticate the Claimant's identity. SOURCE: SP 800-63-2
Trojan Horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. SOURCE: CNSSI-4009
Trustworthy System	Computer hardware, software and procedures that— 1) are reasonably secure from intrusion and misuse; 2) provide a reasonable level of availability, reliability, and correct operation; 3) are reasonably suited to performing their intended functions; and 4) adhere to generally accepted security procedures. SOURCE: SP 800-32
Validation	Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements). SOURCE: CNSSI-4009

Appendix C—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

AC	Access Control
AO	Authorizing Official
APT	Advanced Persistent Threat
AT	Awareness and Training
AU	Audit and Accountability
BYOD	Bring Your Own Device
CA	Security Assessment and Authorization
CAP	Cross Agency Priority
CC	Common Criteria
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CKMS	Cryptographic Key Management System
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CNSSI	Committee on National Security Systems Instruction
COOP	Continuity of Operations Plan
COTS	Commercial Off The Shelf
CP	Contingency Planning
CSP	Cloud Service Provider
CSRC	Computer Security Resource Center
DES	Data Encryption Standard
DHS	Department of Homeland Security

DRP	Disaster Recovery Plan
FIPS	Federal Information Processing Standard
FIRMR	Federal Resource Management Regulation
FIRST	Forum for Incident Response Teams
FISMA2002	Federal Information Security Management Act
FISMA2014	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
GSSP	Generally Accepted Security Practices
HTTP	Hypertext Transfer Protocol
IA	Identification and Authentication
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IR	Incident Response
IRM	Information Resource Management
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
ISO	Information Security Officer
ISO	International Organization for Standardization
ISE	Information Security Engineer
IT	Information Technology
ITL	Information Technology Laboratory
MA	Maintenance
MAC	Message Authentication Code
MP	Media Protection
NIST	National Institute of Standards and Technology

NVD	National Vulnerability Database
OMB	Office of Management and Budget
P.L.	Public Law
PBX	Private Branch Exchange
PE	Physical and Environmental Security
PGP	Pretty Good Privacy
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PL	Planning
PM	Project Management
PS	Personnel Security
RA	Risk Assessment
RAID	Random Array of Inexpensive Disks
RMF	Risk Management Framework
S/MIME	Secure/Multipurpose Internal Mail Extension
SA	Systems and Services Acquisition
SAOP	Senior Agency Official for Privacy
SC	System and Communications Protection
SI	System and Information Protection
SISO	Senior Information Security Officer
SMTP	Simple Mail Transfer Protocol
SP	Special Publication
TCB	Trusted Computing Base